Př. Najděte $\forall$ hom. $\Sigma_3 \Rightarrow (\mathbb{Z}_6, +)$

$$\Sigma_3 = \langle \{(1,2), (2,3)\} \rangle$$

$\forall$ hom. z Σ_3 je jednoznačně určen hodnotami na $(1,2)$ a $(2,3)$

$f : \Sigma_3 \Rightarrow \mathbb{Z}_6$

Víme $\operatorname{ord} f((1,2)) \mid \operatorname{ord}((1,2)) = 2$

$\mathbb{Z}_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
ord	1	6	3	2	3	6

4 případy:

f_{00}: $(1,2) \mapsto [0]_6$

$(2,3) \mapsto [0]_6$

$f(\Sigma_3) = [0]_6$ je homomorfismus

f_{03}: $\underline{(1,2) \mapsto [0]_6}$ $\quad \underline{(2,3) \mapsto [3]_6}$

$f(\underbrace{(1,2,3)}_{\text{řád } 3}) = f((1,2) \circ (2,3)) =$

$= f((1,2)) + f((2,3)) = [0]_6 + [3]_6 = \underbrace{[3]_6}_{\text{řád}}$

$2 \nmid 3 \Rightarrow$ nelze rozšířit na hom.

$\underset{\underset{[0]_6}{\shortparallel}}{f(id)} = f((1,2,3)^3) = 3 \cdot f((1,2,3)) = 3 \cdot [3]_6 =$

$= [3]_6$

f_{30} $\quad (1,2) \mapsto [3]_6 \qquad (2,3) \mapsto [0]_6$

obdobně jako f_{03} nelze

f_{33} $\quad (1,2) \mapsto [3]_6 \qquad (2,3) \mapsto [3]_6$

$$(1,3) = (1,2)\circ(2,3)\circ(1,2) \mapsto [3]_6 + [3]_6 + [3]_6 = [3]_6$$

$$(1,2,3) = (1,2)\circ(2,3) \mapsto [3]_6 + [3]_6 = [0]_6$$

$$(3,2,1) = (2,3)\circ(1,2) \mapsto [0]_6$$

$$\mathrm{id} \mapsto [0]_6$$

je homomorf.

Př. Najděte $\forall$ automorfismy $(\mathbb{Z},+)$

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

záleží jen $f(1)$

nechť $\underline{c = f(1)}$

lze rozšířit na homomorfismus

$$f(k) = c \cdot k$$

Jádro

$$\operatorname{Ker} f = \{a \in \mathbb{Z},\ f(a) = 0\}$$

$$c \neq 0 \Rightarrow \operatorname{Ker} f = \{0\}$$

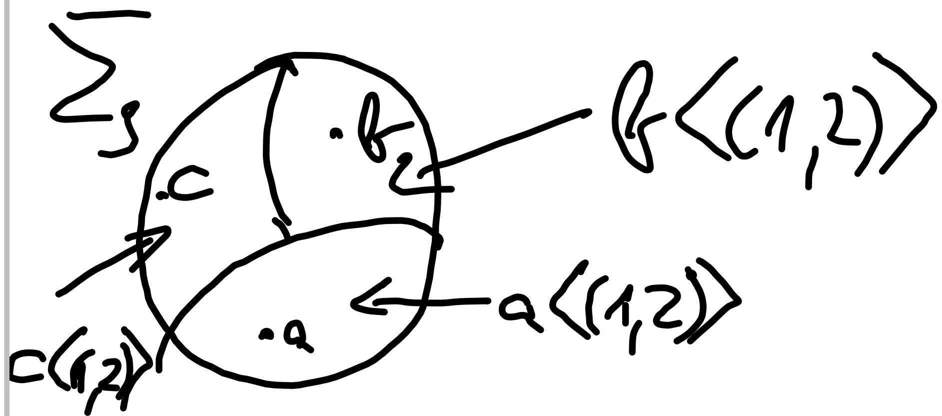
$$c = 0 \Rightarrow \operatorname{Ker} f = \mathbb{Z}$$

Obraz

$$f(\mathbb{Z}) = \{c \cdot k,\ k \in \mathbb{Z}\} = c \cdot \mathbb{Z}$$

Př Popište $\Sigma_3/\langle(1,2)\rangle$

$$\Sigma_3/\langle(1,2)\rangle = \{a\langle(1,2)\rangle,\ a\in\Sigma_3\}$$



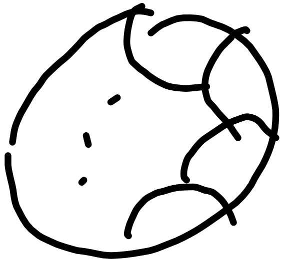
$\langle(1,2)\rangle = \{id, (1,2)\}$

$a = id \quad a\cdot\langle(1,2)\rangle = \{id,(1,2)\} = \langle(1,2)\rangle$

$b = (1,3) \quad b\cdot\langle(1,2)\rangle = \{(1,3)\circ id, (1,3)\circ(1,2)\} = \{(1,3), (1,2,3)\}$

$c = (2,3) \quad c\cdot\langle(1,2)\rangle = \{(2,3)\circ id, (2,3)\circ(1,2)\} = \{(2,3), (1,3,2)\}$

Př. Popište $(\mathbb{C},+)/(\mathbb{R},+)$



$$a+\mathbb{R} = b+\mathbb{R}$$

$$\Updownarrow$$

$$a-b\in\mathbb{R}$$

$$a=(x+iy) \qquad b=(z+iw)$$

$$a-b\in\mathbb{R} \Leftrightarrow y=w$$

$$(\mathbb{C},+)/(\mathbb{R},+) = \{\underbrace{\{x+iy\,;\ x\in\mathbb{R}\}}_{\text{třída všech kompl. čísel s imag. částí } y}\,;\ y\in\mathbb{R}\}$$

Př. Kolik tříd obsahuje Σ_7/H, kde $H = \langle (1,2) \circ (3,4,5,6,7) \rangle$.

$$|\Sigma_7| = |H| \cdot |\Sigma_7/H|$$

$$\Downarrow$$

$$|\Sigma_7/H| = \frac{|\Sigma_7|}{|H|} = \frac{7!}{\operatorname{ord}(1,2)\circ(3,4,5,6,7)} = \frac{7!}{10} =$$

$$= \frac{\cancel{2}\cdot 3\cdot 4\cdot \cancel{5}\cdot 6\cdot 7}{\cancel{10}} = 3\cdot 4\cdot 6\cdot 7 = 12\cdot 42 = 504$$

Př $9^{2008} \equiv ?\ (\mathrm{mod}\ 17)$

17 prvočíslo

$17 \nmid 9 \Rightarrow 9^{16} \equiv 1\ (\mathrm{mod}\ 17)$

$9^{2008} = 9^{16 \cdot 125 + 8} = (9^{16})^{125} \cdot 9^{8} \equiv 1^{125} \cdot (9^2)^4 \equiv$

$\equiv (-4)^4 \equiv ((-4)^2)^2 \equiv$

$\equiv (-1)^2 = 1\ (\mathrm{mod}\ 17)$

$2008 = 16 \cdot 125 + 8$

40

88

8

Př. Najděte všechny normální podgrupy $(\Sigma_3, \circ)$.

$\{id\} \trianglelefteq \Sigma_3$, $\Sigma_3 \trianglelefteq \Sigma_3$

$|\Sigma_3| = 6 \quad H \leq \Sigma_3 \quad |H|$ dělí 6

2 prvkové podgrupy Σ_3:

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

$\{id,(1,2)\} = \langle (1,2) \rangle \overset{?}{\ntrianglelefteq} \Sigma_3$

$(1,3) \circ (1,2) \circ (1,3) = (2,3) \notin \langle (1,2) \rangle$

není normální

3 prvkové podgrupy Σ_3 ?

$\{id, (1,2,3), (3,2,1)\} \overset{?}{\trianglelefteq} \Sigma_3$

$s \in \Sigma_3, \ t \in \langle (1,2,3) \rangle$

$p(s \circ t \circ s^{-1}) = p(s) \cdot p(t) \cdot p(s^{-1}) =$

$= p(s) \cdot p(s^{-1}) \cdot p(t) = p(\underbrace{s \circ s^{-1}}_{id}) \cdot p(t) = 1 \cdot 1 = 1$

$\Downarrow$

$\Leftarrow s \circ t \circ s^{-1} \in \langle (1,2,3) \rangle$

$\langle (1,2,3) \rangle \trianglelefteq \Sigma_3$

Př. Dokažte že pro G komutativní grupu $H \leq G \Rightarrow H \trianglelefteq G$.

$H \leq (G, \cdot)$

$\forall a \in G, \forall h \in H: \quad a \cdot h \cdot a^{-1} \in H$?

$$a \cdot h \cdot a^{-1} = (a \cdot a^{-1}) \cdot h = 1_G \cdot h = h \in H$$

Tedy $H \trianglelefteq G$ $\square$

$$A_3 = \{id, (1,2,3), (1,3,2)\}$$

$$A_3 \trianglelefteq \Sigma_3$$

$$A_3 \ntrianglelefteq \Sigma_4$$

$$(1,4)\circ(1,2,3)\circ(1,4) = (2,3,4) \notin A_3$$

Př. Nechť $G = GL_n(\mathbb{R})$ (grupa regulárních matic $n \times n$ nad $\mathbb{R}$), $H = SL_n(\mathbb{R})$ (special linear group — grupa matic s determinantem 1).

Uvažme zobrazení $\det : A \mapsto \det(A)$

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

Tedy $\det : (GL_n(\mathbb{R}), \cdot) \to (\mathbb{R} \setminus \{0\}, \cdot)$ je homomorfismus grup.

$$\operatorname{Ker} \det = \{A;\ \det(A) = 1\} = SL_n(\mathbb{R})$$

Proto $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$.

Př. Popište faktorgrupu $(\mathbb{Z},+)/(n\mathbb{Z},+)$.

$\mathbb{Z}/n\mathbb{Z}$

$a \in \mathbb{Z}$ $\quad a + n\mathbb{Z} = \{a + n \cdot k,\ k \in \mathbb{Z}\} =$

$= [a]_n$

$\mathbb{Z}/n\mathbb{Z} = \{[a]_n,\ a \in \mathbb{Z}\} = \mathbb{Z}_n$

Operace je definovaná (jako ve faktorgrupě) jako v $(\mathbb{Z}_n,+)$, proto:

$(\mathbb{Z}/n\mathbb{Z},+) = (\mathbb{Z}_n,+)$

Př. Faktorizujte $(\mathbb{Z},+)\times(\mathbb{Z},+)/H$,

kde $H=\{(m,n) : 6 \mid 2m-n\}$

$a=(x,y)\in \mathbb{Z}\times\mathbb{Z}$, $b=(r,s)$

$a+H=\{(x,y)+(m,n) : 6 \mid 2m-n\}=$

$=\{(x+m,y+n) : 6 \mid 2m-n\}$

$a+H=b+H \iff a-b\in H$

$(x-r,y-s)\in H \iff 2(x-r)-(y-s)$

je násobek 6 $\quad 2x-y\equiv 2r-s \pmod 6$

$(0,1),(0,2),(0,3),(0,4),(0,5),(0,6)$

leží každý v jiné třídě

$\mathbb{Z}\times\mathbb{Z}/H=\{(0,1)+H,(0,2)+H,$

$(0,3)+H,(0,4)+H,(0,5)+H,(0,6)+H\}\cong$

$\cong(\mathbb{Z}_6,+)$

Př. Dokažte, že pro $H \trianglelefteq G$ existuje homomorfismus $f: G \to K$, takový že

$$\ker f = H$$

Uvažme projekci $p: G \to G/H$

$$p(a) \mapsto aH$$

Evidentně p je homom.

$$\ker p = \{a \in G;\ p(a) = 1_{G/H} = H\} = H$$

Tedy p je hledaný homomorfismus