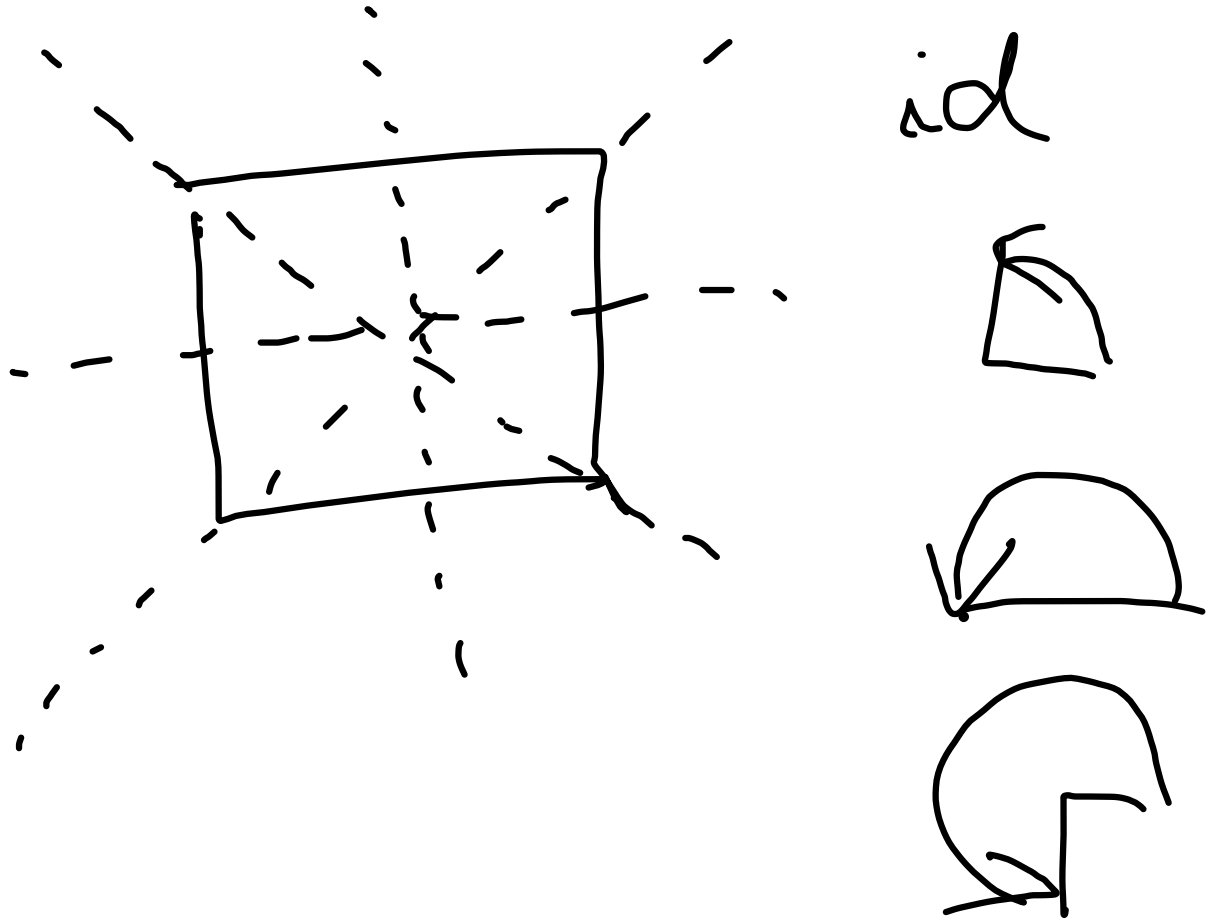
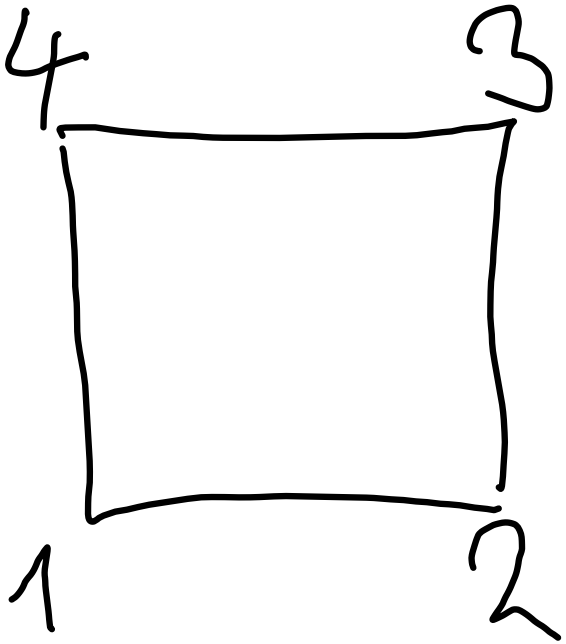

id



D_8

id

$(1,2,3,4)$

$(1,3)\circ(2,4)$

$(1,4,3,2)$

$(1,2)\circ(3,4)$

$(1,4)\circ(2,3)$

$(2,4)$

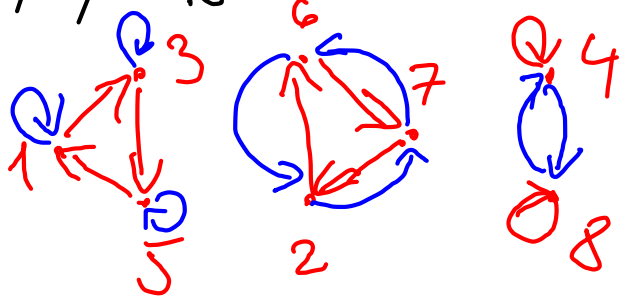
$(1,3)$

$id, (1,2,3,4), (1,3)\circ(2,4), (1,4,3,2), (1,2)\circ(3,4),$
$(1,4)\circ(2,3), (1,3), (2,4)$

1 2 6
$\{id\}\ D_8\ \{id, (1,2)\circ(3,4)\} \ldots$

7 8
$\{(1,3)\circ(2,4), id\}\ \{id, (1,2,3,4),$
$(1,4,3,2), (1,3)\circ(2,4)\}; \{id, (1,3),$ 9
$(2,4), (1,3)\circ(2,4)\}; \{id, (1,2)\circ(3,4),$ 10
$(1,4)\circ(2,3), (1,3)\circ(2,4)\}$

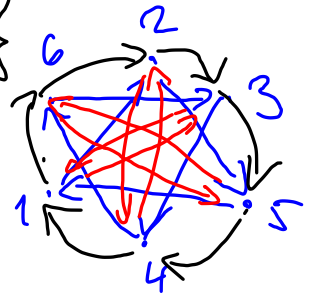
$$M=\{(1,8,2,3,5)\circ(1,2,6,7,8),$$
$$(4,7,6,2)\circ(2,4,8)\}=$$
$$=\{\underbrace{(1,3,5)\circ(2,6,7)}_{\Delta},\ \underbrace{(2,7,6)\circ(4,8)}_{\Lambda}\}$$



$$\langle M\rangle = \{(1,3,5)^a\circ(2,6,7)^b\circ(4,8)^c;\ a,b,c\in\mathbb{Z}\}$$

$$(1,3,5)=\Delta\circ\Lambda^4=(1,3,5)\circ(2,6,7)\circ(2,7,6)^4\circ$$
$$\circ(4,8)^4=(1,3,5)\circ\underbrace{(2,6,7)\circ(2,7,6)}=(1,3,5)$$
$$(2,6,7)=\Lambda^2=[(2,7,6)\circ\underbrace{(4,8)}]^2=(2,6,7)$$
$$(4,8)=\Lambda^3=\underbrace{(2,7,6)^3}\circ(4,8)^3=(4,8)$$

$N = \{(4,5,2,1)\circ(4,6,3,1,5,2);$
$(4,5,2,1)\circ(4,5,6)\circ(2,1,3)\} =$
$= \{\underbrace{(1,2,5)\circ(3,4,6)}_{\Delta}, \underbrace{(1,3)\circ(2,4)}_{1}\circ$
$\underbrace{\circ(5,6)}\}$



$\langle N \rangle \overset{?}{=} \langle \underbrace{(1,6,2,3,5,4)}_{\mu} \rangle = \{(1,6,2,3,5,4)^a;$
$a \in \mathbb{Z}\}$

$\Delta \circ \Delta = (1,2,5)\circ(3,4,6)\circ(1,3)\circ(2,4)\circ(5,6) =$
$= (1,4,5,3,2,6) = \mu^{-1}$

$\mu^3 = (1,6,2,3,5,4)^3 = (1,3)\circ(6,5)\circ(2,4)$

$\mu^2 = (1,6,2,3,5,4)^2 = (1,2,5)\circ(6,3,4) = \Delta$

$GL_2(\mathbb{Z}_2)$ ... general linear group

a

$M = \{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \}$

$\langle M \rangle = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = a^0, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = a^1, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, a \}$

$a^2 = 1_G \quad / \cdot a^{-1} \qquad a^2 \cdot a^{-1} = a^{-1}$

a

$$N = \left\{ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \qquad a^2 = b$$

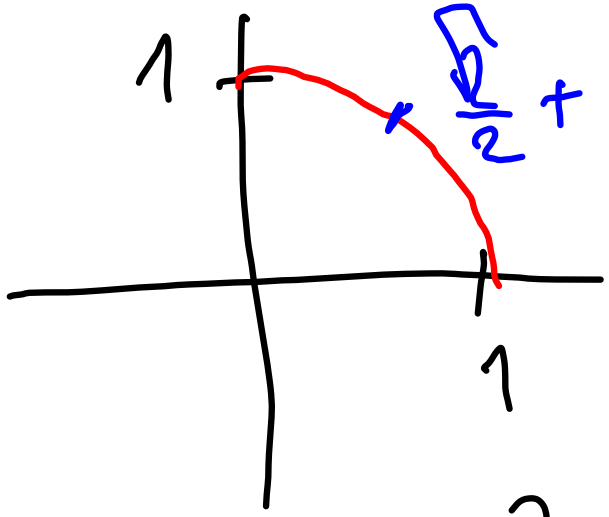
$$a \qquad b \qquad \langle N \rangle = \langle a \rangle$$

$$\langle N \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

$$a^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\langle N \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, a, a^2 \right\}$$



$$\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i = e^{i \cdot \frac{\pi}{4}} = a$$

$$a^8 = e^{8i\frac{\pi}{4}} = e^{2\pi i} = 1$$

$$\langle a \rangle = \{1, a, a^2, a^3, a^4, a^5, a^6, a^7\}$$

$$a = i \qquad a^3 = -1 \qquad a^5 = -i$$

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

$\operatorname{ord} 1 = 1$

$\operatorname{ord} 2 = 3 \quad 2^1 = 2,\ 2^2 = 4,\ 2^3 = 1$

$\operatorname{ord} 3 = 6 \quad 3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,$

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

$$[3]_7 \longmapsto [1]_6$$

$$[3]_7^2 = [2]_7 \mapsto 2 \cdot [1]_6 = [2]_6$$

$\vdots$

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

$\text{ord } 1 = 1$

$\text{ord } 3 = 2$ $\quad 3^1 = 3,\ 3^2 = 1$

$\text{ord } \bar{5} = 2$ $\quad \bar{5}^1 = \bar{5},\ \bar{5}^2 = 1$

$\text{ord } 7 = 2$ $\quad 7^1 = 7,\ 7^2 = 1$

$\mathbb{Z}_8^\times = \langle \{3, \bar{5}\} \rangle$ $\quad (3 \cdot \bar{5} = 7)$

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

ord $\quad 1 \quad 2 \quad 2 \quad 2$

$f: \quad f(3) = (0,1)$

$\quad\quad f(\bar{5}) = (1,0)$

$f(7) = f(3 \cdot \bar{5}) = (0,1) + (1,0) = (1,1)$

$\quad\quad f(1) = (0,0)$

$[a]_{20} = [b]_{20}$

$\Downarrow$ je vždy $f([a]_{20}) = f([b]_{20})$

$\exists k \in \mathbb{Z}: a = 20k + b$

$f([a]_{20}) = f([20k+b]_{20}) =$

$= (1,2,3,4,5)^{20k+b} = (1,2,3,4,5) = f([b]_{20})$

$\forall [c]_{20}, [d]_{20} \in \mathbb{Z}_{20}:$

$f([c]_{20} + [d]_{20}) = f([c]_{20}) \circ f([d]_{20})$

$f([c]_{20} + [d]_{20}) = f([c+d]_{20}) = (1,2,3,4,5)^{c+d}$

$f([c]_{20}) \circ f([d]_{20}) = (1,2,3,4,5)^{c} \circ (1,2,3,4,5)^{d} =$

$= (1,2,3,4,5)^{c+d}$

Tedy f je homomorfismus.

$\operatorname{ord} a = n$ $(G,\circ) \to (H,\cdot)$ n-násl.

$1_H = f(1_G) = f(a^n) = f(\underbrace{a \circ a \circ \dots \circ a}_{n}) =$

$= \underbrace{f(a) \cdot f(a) \cdot \dots \cdot f(a)}_{n} = [f(a)]^n$

$f : (\mathbb{Z}_6, +) \longrightarrow (\Sigma_3, \circ)$

$\operatorname{ord}_{\Sigma_3} f(a) \mid \operatorname{ord}_{\mathbb{Z}_6} a$

ord 1 2 2 2 3 3

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

$\mathbb{Z}_6 = \langle [1]_6 \rangle$

$f_1 : [1]_6 \longmapsto id$

$f_2 : [1]_6 \longmapsto (1,2)$

f_3 — " — $(1,3)$

f_4 — " — $(2,3)$

f_5 $[1]_6 \longmapsto (1,2,3)$

$[4]_6$

$[2]_6, [5]_6 \longmapsto (3,2,1)$

$[3]_6, [6]_6 \longmapsto id$

f_6 — " — $(3,2,1)$

$(1,2,3)$