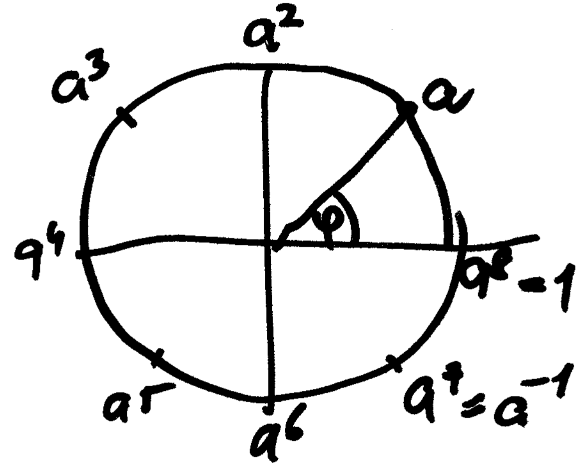
9) $G = (\mathbb{C}^*, \cdot)$

$a = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$

$|a| = \sqrt{\frac{1}{2} + \frac{1}{2}} = 1$

$\cos\varphi = \frac{\sqrt{2}}{2}$

$\varphi = \frac{\pi}{4}$



$\langle a \rangle = \{1, a, a^2, \dots, a^7 = a^{-1}\}$

a řádu 8 v G

---

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

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

$|\Sigma_3| = 6$

$\mathbb{Z}_6$: $[0]$, $[1]$, $[2]$, $[3]$, $[4]$, $[5]$

- f_{00}: $(1,2) \mapsto [0]$, $(1,3) \mapsto [0]$ $\quad \forall g \in \Sigma_3 : f_{00}(g) = [0]$
- f_{10} $(1,2) \mapsto [1]$, $(1,3) \mapsto [0]$ $\Rightarrow (1,2)\circ(1,2) \mapsto [1] + [1]$
  $\quad\quad id \mapsto [2]$
  není homom.

f_{30}:

$(1,2) \mapsto [3]$

$(1,3) \mapsto [0]$

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

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

$id \mapsto [0]$

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

je homom.

f_{03}:

$(1,2) \mapsto [0]$

$(1,3) \mapsto [3]$

dopočítat analogicky

f_{33}:

$(1,2) \mapsto [3]$

$(1,3) \mapsto [3]$

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

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

$id \mapsto [0]$

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

je homo

řád f(a) dělí řád a

řád $f(a)$ dělí $\underbrace{\text{řád } a}_{n}$:

$$\underline{(f(a))^n} = f(a^n) = f(e) = e$$

$\Rightarrow$ řád $f(a)$ dělí n.

---

(11) $(\mathbb{Z}_7^\times, \cdot) \cong (\mathbb{Z}_6, +)$

$f: (\mathbb{Z}_6, +) \to (\mathbb{Z}_7^\times, \cdot)$

$[1] \mapsto$ $[1]$ ... triviální

$[2]$ není bijekce $([3] \mapsto [2^3]$

$[3]$

$[a]$	1	2	3	4	5	6
$g([a])$	5	4	6	2	3	1

izomorfismus

$[a]$	1	2	3	4	5	6
$f([a])$	$3 = 3^1$	$2 = 3^2$	$6 = 3^3$	4	5	1

bijekce $\Downarrow$ izomorfismus

11b $(\mathbb{Z}_8^\times, \cdot) \cong (\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$

$[1], [3], [5], [7]$ $\quad ([0],[0]), ([0],[1]), ([1],[0]), ([1],[1])$

řády $\quad 1 \quad 2 \quad 2 \quad 2 \qquad 1 \quad 2 \quad 2 \quad 2$

$[3] \mapsto ([0],[1])$

$[5] \mapsto ([1],[0])$ JE IZOMORFISMUS

$[3]\cdot[5] \mapsto ([1],[1])$

$[1] = [3]\cdot[3] \mapsto ([0],[0])$

---

12 $(m,k)=1 \quad (\mathbb{Z}_{mk},+) \cong (\mathbb{Z}_m,+)\times(\mathbb{Z}_k,+)$

$[1] \longmapsto ([1],[1])$

$\mathbb{Z}_{20} \to \mathbb{Z}_4 \times \mathbb{Z}_5$

$1 \mapsto (1,1)$

$2 \mapsto (2,2)$

$3 \mapsto (3,3)$

$4 \mapsto (0,4)$

$5 \mapsto (1,0)$

$6 \mapsto (2,1)$

$7 \mapsto (3,2)$

$8 \mapsto (0,3)$

$9 \mapsto (1,4)$

$10 \mapsto (2,0)$

$11 \mapsto (3,1)$

$12 \mapsto (0,2)$

$13 \mapsto (1,3)$

$14 \mapsto (2,4)$

$15 \mapsto (3,0)$

$16 \mapsto (0,1)$

$17 \mapsto (1,2)$

$18 \mapsto (2,3)$

$19 \mapsto (3,4)$

$20 \mapsto (0,0)$

13) 1. $\mathbb{Z}_2 \times \mathbb{Z}_5 \to \mathbb{Z}_{10}$ $f([a],[b]) = [a+b]$

$a_1 \equiv a_2 (2)$
$b_1 \equiv b_2 (5)$ $\overset{?}{\Longrightarrow}$ $a_1+b_1 \equiv a_2+b_2 \pmod{10}$

$a_1 = a_2 = 0$ $b_1 = 5$, $b_2 = 0$ $\wedge$ $0+5 \not\equiv 0+0$ (1

$\lightning$ není zobrazení

2. $\mathbb{Z}_2 \times \mathbb{Z}_5 \to \mathbb{Z}_{10}$ $g([a],[b]) = [5a+2b]$

$a_1 \equiv a_2 (2)$
$b_1 \equiv b_2 (5)$ $\overset{?}{\Longrightarrow}$ $5a_1+2b_1 \equiv 5a_2+2b_2$ (mod

$2 \mid a_1 - a_2$
$5 \mid b_1 - b_2$ $\to 10 \mid 5(a_1-a_2)+2(b_1-b_2)$ ✓

JE TO ZOBRAZENÍ

o homomorfismus?:

$g([a_1,b_1]+[a_2,b_2]) = g([a_1]+[a_2],[b_1]+[b_2]) \overset{?}{=} g([a_1],[b_1]) + g([a_2],[b_2])$

$[5(a_1+a_2)+2(b_1+b_2)]_{10} \overset{?}{=} [5a_1+2b_1] + [5a_2+2b_2]$ ✓ homom

(13) poz.:

g izom.? stačí surjekce (příp. injekce), tj. ex.

$a, b : 5a + 2b \equiv 1 \pmod{10}$

$a = 1, b = -2$

$g([1], [3]) = [5 \cdot 1 + 2 \cdot 3] = [1]$

$\Rightarrow$ surjektivní $\Rightarrow \ker g = \{([0], [0])\}$

---

3. $h : (\mathbb{Z}_4, +) \to (\mathbb{C}^*, \cdot)$ $\quad h([a]_4) = i^a$

zobr. $a \equiv b \, (4) \overset{?}{\Rightarrow} i^a = i^b$

$a = b + 4 \cdot k, k \in \mathbb{Z} \Rightarrow i^a = i^{b+4 \cdot k} = i^b \cdot (i^4)^k = i^b \cdot 1^k = i^b$ ✓

hom. : $h([a] + [b]) \overset{?}{=} i^a \cdot i^b$

$\overset{\shortparallel}{i^{a+b}} = i^a \cdot i^b$ ✓

není izom.

$\ker h = \{[a] \in \mathbb{Z}_4 ; i^a = 1\} = \{[0]\}$

13 pokr.

4. $(\mathbb{Z}_5, +) \to (\mathbb{C}^*, \cdot)$ $\quad k(\{a\}_5) = i^a$

zobrazení?: $a \equiv b (5) \Rightarrow i^a = i^b$

$a = 5$, $b = 0$ $\Rightarrow$ $\left.\begin{array}{l} i^a = i^5 = i \cdot i^4 = i \\ i^0 = 1 \end{array}\right\} 1 \neq i$

NENÍ!

5. $l : \Sigma_6 \to \Sigma_6$ $\quad l(s) = s^2$

zobrazení ano, homom.: $l(s \circ t) \stackrel{?}{=} l(s) \circ l(t)$

$(s \circ t)^2 \stackrel{?}{=} s^2 \circ t^2$

$s = (1,2)$ $\quad s^2 = id$

$t = (1,3)$ $\quad t^2 = id$

$s \circ t \circ s \circ t = s \circ s \circ t \circ t$

$s \circ t = (1,3,2)$ $\quad (s \circ t)^2 = (1,2,3) \neq s^2 \circ t^2$

NENÍ HOMOMORFISMUS

6. $m : \Sigma_6 \to \Sigma_6$ $\quad m(s) = (1,2) \circ s \circ (1,2)$ $\quad id$

zobr. ANO, hom: $m(s \circ t) = (1,2) \circ s \circ t \circ (1,2) \stackrel{!}{=} (1,2) \circ s \circ \underline{(1,2) \circ (1,2)} \circ t \circ (1,2) = m(s) \circ m(t)$

ANO

(13) 6. dok. $m(s) = (1,2) \circ s \circ (1,2)$

stačilo by dokázat buď injektivitu nebo surjektivitu:

inj. $m(s) = m(t) \Rightarrow (1,2) \circ s \circ \cancel{(1,2)} = (1,2) \circ t \circ \cancel{(1,2)}$ | L $(1,2)$, P $(1,2)$

$s = t \Rightarrow$ injektivní

surj.: $\forall t \in \Sigma_6 \ \exists s \in \Sigma_6 : m(s) = t$

$(1,2) \circ s \circ (1,2) = t$ | L $(1,2)$, P $(1,2)$

$$\underline{\underline{s = (1,2) \circ t \circ (1,2)}}$$

(14) $f: G \to G$

$x \mapsto x^{-1}$

homom.: $f(x\cdot y) \overset{?}{=} f(x)\cdot f(y)$

$(x\cdot y)^{-1} \overset{?}{=} x^{-1}\cdot y^{-1}$

$y^{-1}\cdot x^{-1} \overset{?}{=} x^{-1}\cdot y^{-1}$ platí $\forall x,y \in G \iff G$ je komutativní

f bijekce zřejmé: $x^{-1} = y^{-1} \Rightarrow \underbrace{(x^{-1})^{-1}}_{x} = \underbrace{(y^{-1})^{-1}}_{y}$ — injektivní

surjektivní: $y \in G$ lib. $\Rightarrow f(y^{-1}) = (y^{-1})^{-1} = y$ ✓

(15) $(\mathbb{C},+)/(\mathbb{R},+) = \{a+\mathbb{R} \,;\, a \in \mathbb{C}\}$

kdy $a+\mathbb{R} = b+\mathbb{R} \iff a-b \in \mathbb{R}$ $\left(\begin{matrix} a = x+iy \\ b = u+iv \end{matrix}\right) \iff y = v$

$(\mathbb{C},+)/(\mathbb{R},+) = \{\, \{x+iy \,;\, \overset{x\in\mathbb{R}\text{ lib.}}{y = \text{konst.}}\} \,,\ \text{konst.} \in \mathbb{R} \}$

16) počet tříd rozkladu?

$$|G| = |H| \cdot |G/H| = |H| \cdot \underbrace{[G:H]}_{?\ \text{index } H \text{ v } G}$$

$|G| = 7!$

$|H| =$ řád prvku $\underbrace{(1,2)\circ(3,4,5,6,7)}_{a}$ v S_7

$a^2 = id \circ (3,5,7,4,6)$

$a^3 = (1,2)^3 \circ (3,4,5,6,7)^3 = (1,2)\circ(3,6,4,7,5)$

$a^4 = id \circ (3,7,6,5,4)$, $a^5 = (1,2)\circ id \Rightarrow a^{10} = id$

[$a^2, \dots, a^9 \neq id$, neboť $a^n = id \iff$ řád a dělí n

pro nás tedy řád a dělí 10]

$$\Rightarrow [G:H] = \frac{7!}{10} = 3\cdot 4\cdot 6\cdot 7 = 504$$