

HOMOMORFISMUS:
 máme grupy (G, \cdot) , (H, \square)
 Zobrazení $f: G \rightarrow H$ nazýváme
 homomorfismus, pokud $\forall a, b \in G$
 platí, že

$$f(a \cdot b) = \underbrace{f(a)}_{\in H} \square \underbrace{f(b)}_{\in H}$$

3 15-16:01

PŘ.: $\varphi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$
 $\varphi(a) = 2a$
 Homomorfismus? ANO!
 $a, b \in \mathbb{Z}$
 $f(a+b) = 2(a+b)$
 $f(a) + f(b) = 2a + 2b = 2(a+b)$ } \ominus

3 15-16:05

PŘ.: (G, \cdot) ANO
 $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}$
 $f: (G, \cdot) \rightarrow (\mathbb{Z}, +)$ $f(A) = a - c$
 $A, B \in G$
 $f(A \cdot B) = f\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \right) =$
 $= f\left(\begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix} \right) = a+d-f-c$
 $f(A) + f(B) = f\left(\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right) + f\left(\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \right) =$
 $= a-c + d-f = a+d-f-c$ } \ominus

3 15-16:08

$M \rightarrow N$ $N \rightarrow \mathbb{Z}$
 $1 \mapsto 2$
 $2 \mapsto 1$
 $\forall a, b \in M, a \neq b: f(a) + f(b) \in \mathbb{N}$
 SURJEKTIVNÍ
 $\forall m \in \mathbb{N} \exists a \in M: f(a) = m$
 BIJEKCE = SURJEKCE & INJEKCE
 $\mathbb{Z} \rightarrow \mathbb{N}_0$
 $\mathbb{Z}^+ \rightarrow \mathbb{Z}$
 $\mathbb{Z}^- \rightarrow \mathbb{Z}^+$
 $0 \mapsto 0$

3 15-16:15

JÁDRO: $f: G \rightarrow H$ hom
 $\text{Ker } f = \{g \in G \mid f(g) = e_H\} \in G$
 OBRAZ: $f: G \rightarrow H$
 $\text{Im } f = \{h \in H \mid \exists g \in G: f(g) = h\} \in H$
 VĚTA: Hom f je INJ $\Leftrightarrow \text{Ker } f = \{e_G\}$
 DEF: Izomorfismus je bijektivní homomorfismus.

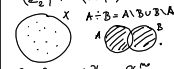
3 15-16:20

PŘ.: $\pi: (\mathbb{R}^2, +) \rightarrow (\mathbb{R}, +)$
 $\pi(x, y) = x$
 hom? jádro? obraz?
 $\pi((x, y) + (\bar{x}, \bar{y})) = \pi(x + \bar{x}, y + \bar{y}) =$
 $= x + \bar{x}$ } \ominus
 $\pi(x, y) + \pi(\bar{x}, \bar{y}) = x + \bar{x}$
 Jádro: $\text{Ker } \pi = \{(x, y) \mid \pi(x, y) = 0\}$
 $= \{(0, a) \mid a \in \mathbb{R}\}$
 Obraz: $\text{Im } \pi = \{x \in \mathbb{R} \mid \exists (u, v): \pi(u, v) = x\}$
 $\text{Im } \pi = (\mathbb{R}, +)$
 projekce na 1. složku.

3 15-16:25

PR: $(\mathbb{Z}_{15}, +) \rightarrow (\mathbb{Z}_3, +) \times (\mathbb{Z}_5, +)$
 $\varphi([a]_{15}) = ([2a]_3, [2a]_5)$
 zobrazení? Homomorfismus?
 KOREKTNOST = meziarisi ma
 nako reprezentacni.
 $[a]_{15} = [a+15]_{15}$
 $\varphi([a]_{15}) = ([2a]_3, [2a]_5)$
 $\varphi([a+15]_{15}) = ([2(a+15)]_3, [2(a+15)]_5) =$
 $= ([2a+30]_3, [2a+30]_5) =$
 $= ([2a]_3, [2a]_5)$
 Xmo: ANO!
 $\varphi([a]_{15}, [b]_{15}) = \varphi([a+b]_{15}) = ([2(a+b)]_3, [2(a+b)]_5)$
 $\varphi([a]_{15}) + \varphi([b]_{15}) = ([2a]_3, [2a]_5) + ([2b]_3, [2b]_5) =$
 $= ([2a+2b]_3, [2a+2b]_5)$

3 15-16:32

PR: Ukaže, že
 $(\mathbb{Z}_n, +) \cong (\mathbb{P}(n), +)$

 $\mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n^2$
 $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$
 $|x| = n$
 $A = \{0, 1, \dots, n-1\}$
 $0 \dots a, b, \dots$
 $\varphi: A \rightarrow (a)_i, \varphi: B(x) \rightarrow \mathbb{Z}_n^2$
 $\varphi(A+B) = \varphi(A) + \varphi(B)$ zřejmé!
 Pokud prvek n není v obou množinách, pak n obou násobí
 φ na n-tém místě.
 Symetrický rozdíl A+B rozdělí
 a n násobí na n-tém místě
 φ(A+B) = B.
 202
 N.J.: $f(A) + f(B) \stackrel{?}{=} A+B$
 $(a)_i = (b)_i, a_i = b_i, f: i \rightarrow a+b$
 $\Rightarrow a=b$
 SUR.: $(a)_i$
 Oba množiny mají stejný počet prvků, protože jsou symetrický rozdíl množin A, B: $\varphi(A) = \varphi(B)$.
 INJEKCE POMOCI JABEA:
 Ker φ = {0} ∩ {0} = {0} = (0, 0, ..., 0)
 $= \{0\} \Rightarrow$ INJ

3 15-16:43

PR: $h: (\mathbb{Z}_4, +) \rightarrow (\mathbb{Z}_5, +)$
 $h(1) = (2, 3) \circ \rho(2, 3)$
 Homomorfismus? ANO
 $a, b \in \mathbb{Z}_4$
 $h(\rho \circ 1) = (2, 3) \circ \rho \circ 1(2, 3)$
 $h(\rho) \circ h(1) = (2, 3) \circ \rho \circ (2, 3) \circ (2, 3) \circ 1 \circ (2, 3) =$
 $= (2, 3) \circ \rho \circ 1(2, 3)$

3 15-17:03

DEF: Řád grupy (G, \cdot)
 je počet jejích prvků.
 Řád prvku $a \in (G, \cdot)$ je nejmenší
 $n \in \mathbb{N}$ takové, že $a^n = e_a$.

PLATI: Řád prvku dělí
 řád grupy !!!

3 15-17:09

PR: $(\mathbb{Z}_{81}^x, \cdot)$ a) řád grupy
 b) prvek řádu 9 a 10

a) $|\mathbb{Z}_{81}^x| = \varphi(81) = \varphi(3^4) = 2 \cdot 3^3 = 54$

b) prvek řádu 10 \nexists , neboť $10 \nmid 54$.

ord $[2]_{81} \stackrel{?}{=} 9$
 $2^0 = 1$
 $2^1 = 2$
 $2^2 = 4$
 $2^3 = 8$
 $2^4 = 16$
 $2^5 = 32$
 $2^6 = 64 \equiv 17$
 $2^7 = 17 \cdot 2 = 34$
 $2^8 = 34 \cdot 2 = 68$
 $2^9 = 68 \cdot 2 = 136 \equiv 13 \pmod{81}$
 $\in \mathbb{N}$!

ord $[5]_{81} \stackrel{?}{=} 9$
 $5^0 = 1$
 $5^1 = 5$
 $5^2 = 25$
 $5^3 = 125 \equiv 44$
 $5^4 = 44 \cdot 5 \equiv 58 \equiv -23$
 $5^5 = -23 \cdot 5 = -115 \equiv -34$
 $5^6 = -34 \cdot 5 = -170 \equiv -89$
 $5^7 = -89 \cdot 5 = -445 \equiv -364$
 $5^8 = -364 \cdot 5 = -1820 \equiv -1009$
 $5^9 = -1009 \cdot 5 = -5045 \equiv -4964$
 $\pmod{81}$

3 15-17:11

PR: Ukaže racionální homomor-
 fismy $\mathbb{Z}_{15} \rightarrow \mathbb{Z}_{24}$

$\mathbb{Z}_{15} \dots 1, 3, 5, 15$
 $\mathbb{Z}_{24} \dots 1, 2, 3, 4, 6, 8, 12, 24$

PLATI: Řád obrazu dělí
 řád prvku!
 f zobr. $\frac{\text{ord } f(a)}{\text{ord } a}$

1) $\mathbb{Z}_{15} \rightarrow \mathbb{Z}_{24}$
 $\varphi([a]_{15}) = f([a]_{15}) = [0]_{24}$

2) řád 1 ... $[0]_{24}$
 řád 3 ... $[16]_{24}$

1 $\rightarrow 8_{24}$ 5 $\rightarrow 16_{24}$ 8 $\rightarrow 16$ 12 $\rightarrow 0$
 2 $\rightarrow 16_{24}$ 6 $\rightarrow 0_{24}$ 9 $\rightarrow 0$ 13 $\rightarrow 8$
 3 $\rightarrow 0_{24}$ 7 $\rightarrow 8_{24}$ 10 $\rightarrow 8$ 14 $\rightarrow 16$
 4 $\rightarrow 8_{24}$ 11 $\rightarrow 16$ 0 $\rightarrow 0_{24}$

3 15-17:22



3 15-17:34