12.1 (i) $\varphi: \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$

$$\varphi([a]_4, [b]_3) = [a-b]_{12}$$

- je tato definice φ korektní?

$[1]_3 = [4]_3 = [7]_3$ apod.

$$\varphi([1]_4, [4]_3) = [1-4]_{12}$$

$$\| \qquad = [9]_{12} \not\to$$

$$\varphi([1]_4, [1]_3) = [0]_{12}$$

$\Rightarrow$ φ není korektně definována

(ii) $\varphi: \mathbb{Z}_4 \times \mathbb{Z}_3 \to \mathbb{Z}_{12}$

$$\varphi([a]_4, [b]_3) = [6a+4b]_{12}$$

- $\varphi([a]_4, [b]_3) =$

$$= \varphi([a+4k]_4, [b+3\ell]_3)$$

$$\downarrow$$

$$= [6(a+4k) + 4(b+3\ell)]_{12} =$$

$$= [6a + 24k + 4b + 12\ell]_{12}$$

$$= [6a + 4b]_{12}$$

$\Rightarrow$ nezávisí na $k, \ell \Rightarrow$
je korektně definováno

- **homo grupy**

$x = ([a]_4, [b]_3) \quad y = ([c]_4, [d]_3)$

chceme uhrad, že

$\varphi(x+y) = \varphi(x) + \varphi(y)$

$\hookrightarrow$ v $\mathbb{Z}_4 \times \mathbb{Z}_3 \quad \hookrightarrow$ v $\mathbb{Z}_{12}$

$$\varphi(x+y) = \varphi(([a]_4, [b]_3) + ([c]_4, [d]_3))$$

$$= \varphi([a+c]_4, [b+d]_3) =$$

$= [6(a+c) + 4(b+d)]_{12}$

$\varphi(x) + \varphi(y) = [6a+4b]_{12} + [6c+4d]_{12}$

$= [6(a+c), 4(b+d)]_{12}$ //

$\Rightarrow$ je to komu grup

Neutr. prvek: $\varphi([0]_4, [0]_3) = [0]_{12}$

Jádro: $\varphi(x) = 0$

$\varphi([a]_4, [b]_3) = [6a + 4b]_{12}$

$6a + 4b = 12\ell \qquad a, b, \ell \in \mathbb{Z}$

$3a + 2b = 6\ell$

$\hookrightarrow$ 3 | b $\Rightarrow b = 3b_1$

2 | a $\qquad a = 2a_1$

$\Rightarrow 3 \cdot 2a_1 + 2 \cdot 3b_1 = 6\ell$ platí vždy

• Jádro je $\{([0]_4, [0]_3), ([7]_4, [0]_3)\}$

$\cong$

je dvouprvkové $\cong \mathbb{Z}_2$ $\cong \mathbb{Z}_4 \times \mathbb{Z}_3$

$\Rightarrow$ obraz má 6 prvků

$\cong$

$\mathbb{Z}_{12}$

Obraz: $\{[0]_{12}, [7]_{12}, [4]_{12}, \dots, [10]_{12}\}$

$\cong$ $\cong$

$\mathbb{Z}_{12}$

$\cong \mathbb{Z}_6$

• injektivita: není

(netriviální jádro)

• surjektivní není

(iii) $\varphi([a]_4, [b]_3) = [0]_{12}$

- bine definită
- morfism de grupuri
- $\ker \varphi = \mathbb{Z}_4 \times \mathbb{Z}_3$

  ↳ nucleu

  $\operatorname{Im} \varphi = \{[0]_{12}\}$

  ↳ nucleu

- nici inj. nici surj.

12.2 (ii) $\varphi : \mathbb{Z}_4 \to \mathbb{C}^*$

$$\varphi([a]_4) = i^a$$

- $\varphi([a+4k]) = i^{(a+4k)} =$

$$= i^a \cdot i^{4k} = i^a \cdot (i^4)^k =$$

$$= i^a \cdot \underbrace{1^k}_{=1} = i^a \quad \text{Ok}$$

- morfism de grupuri

$$\varphi([a]_4 + [b]_4) = \varphi([a+b]_4)$$

$$= i^{a+b} = i^a \cdot i^b = \checkmark$$

$$\varphi([a]_4) \cdot \varphi([b]_4) = i^a \cdot i^b$$

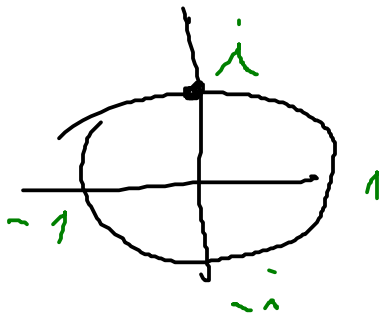
Neutr. prve v. : $\varphi([0]_4) = i^0 = 1$

neutr. prvek v $\mathbb{Z}$ — neutr. prvek v $\mathbb{C}^*$

· Jádro:

$$\varphi([a]_4) = 1$$

$$i^a = 1$$



$$\Rightarrow 4 \mid a \Rightarrow$$

$$[a]_4 = [0]_4$$

$\Rightarrow$ hledám jádro

$$\{[0]_4\} = \ker \varphi$$

Obrat:

$$\mathrm{Im}(\varphi) = \{1, i, i^2 = -1, i^3 = -i\}$$

$\parallel$ (2) $\cap$ (1)

$\mathbb{Z}_4$ $\quad\quad$ $\mathbb{C}^*$

(ii) $\varphi : \mathbb{Z}_5 \longrightarrow \mathbb{C}^*$

$$\varphi([a]_5) = i^a$$

- $[0]_5 = [5]_5$

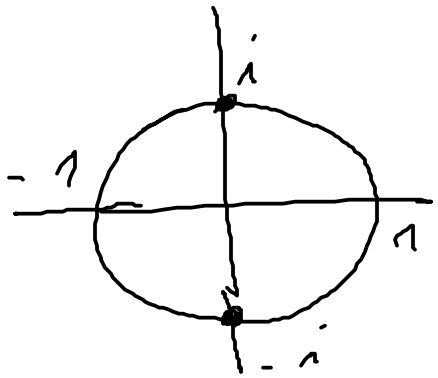
$\varphi \downarrow$ $\quad\quad$ $\varphi \downarrow$

$i^0 = 1$ $\quad\quad$ $i^5 = i^4 \cdot i = i$ ($i^4 = 1$)

$\Rightarrow$ není korektně definováno

- $\varphi : \mathbb{Z}_4 \longrightarrow \mathbb{C}^*$

$$\varphi([a]_4) = (-i)^a$$



korektno def,
homo grup

Jádro $\varphi([0]_4) = 1 = (-i)^a$

$a \in \mathbb{Z}_4 \Rightarrow [a]_4 = [0]_4$

$\Rightarrow$ jádro trivialní

- je injektivní
- není surjektivní

(IV) $\varphi : \mathbb{Z} \to \mathbb{C}^*$

$\varphi(a) = i^a$

- je to homo grup
- Jádro: $\ker \varphi = \{a = 4n \mid n \in \mathbb{Z}\}$

$\hookrightarrow$ není inj

Obraz : $\{1, i, -1, -i\} \subseteq \mathbb{C}^*$

$\cong$

$\mathbb{Z}_4$

Lineární kódy

Kódy

12.3 (5,3) kód nad $\mathbb{Z}_2$

Generovací polynom

$p(x) = x^2 + x + 1$

Slova před zakódováním : 000, 001, 010, 011
100, 101, 110, 111

Kódování polynomu $v(x)$:

$$x^2 v(x) = q(x)p(x) + e(x) \quad (*)$$

kódové slovo

dělení se zbytkem

Výpis kódových slov =

= výpis násobků $p(x)$:

$0 \cdot p(x) = 0$ — 00000

$1 \cdot p(x) = x^2 + x + 1$ — 11100

$x \cdot p(x) = x^3 + x^2 + x$ — 01110

$(x+1)p(x) = x^3 + 1$ — 10010

$x^2 \cdot p(x) = x^4 + x^3 + x^2$ — 00111

$(x^2 + x) \cdot p(x) = x^4 + x$ — 01001

$(x^2 + 1) \cdot p(x) = x^4 + x^3 + x + 1$ — 11011

$(x^2 + x + 1)\, p(x) = x^4 + 1$ — 10001

(*) kódovým

$v(x) \mapsto x^2 \cdot v(x) + e(x)$

kódování je zobrazení
$\varphi: (\mathbb{Z}_2)^3 \to (\mathbb{Z}_2)^5$, které je
lineární

je určeno maticí
zapíšeme v bázi $1, x, x^2$

$1 \mapsto 100$ $\quad x \mapsto 010$ $\quad x^2 \mapsto 001$

$1 \mapsto x^2 \cdot 1 = x^2 = \underbrace{(x^2+x+1)}_{r(x)} + \underbrace{(x+1)}_{e(x)}$

$\boxed{1 \longmapsto x^2+x+1}$

$x \mapsto x^2 \cdot x = x^3 = \underbrace{(x+1)(x^2+x+1)}_{} + 1$

$x^3 = x(x^2+x+1) + (x^2+x+1) + 1$

$= (x+1)(x^2+x+1) + 1$

$\boxed{x \longmapsto x^3+1}$

$x^3 + x^2 + x + x^2 + x + 1 =$

$= x^3 + 1$

$x^2 \rightsquigarrow x^2 \cdot x^2 = x^4 = (x^2+x)(x^2+x+1)+x$

$x^4 = x^2(x^2+x+1) + x^2+x$

$= x^2(x^2+x+1) + x(x^2+x+1) + x$

$x^2 \mapsto x^4+x$

x^4+x

$$G = \left(\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)$$

generująca

$(\mathbb{Z}_2)^3 \to (\mathbb{Z}_2)^5$

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

macierz kontroli parzystości $(\mathbb{Z}_2)^5 \to (\mathbb{Z}_2)^2$

→ detekuje chybná slova

$$H \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$