71) $(G,\cdot)$ grupa, $Aut(G)$

$\varphi: G \to G$, izomorf. .... automorfism

$(Aut(G), \circ)$ je grupa?

1) asoc. $f, g, h: G \to G$

$f \circ (g \circ h) \stackrel{?}{=} (f \circ g) \circ h$ ANO – skládání zobrazení $G \to G$

2) neutr. prvek:

$f \circ e = f$ & $e \circ f = f$ .... $e = ID_G$

3) inverze ke f

$f \circ h = ID$ & $h \circ f = ID$

inverze k f je $h = f^{-1}$ ... existuje vždy neboť f je bijekce.

A) $(Aut(\mathbb{Z}_8^\times), \circ)$

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

Izomorfismus zachovává řády!

$ord_8 1 = 1$

$ord_8 3 = 2$

$ord_8 5 = 2$

$ord_8 7 = 2$

1) $1_8 \mapsto 1_8$, $3_8 \mapsto 5_8$, $5_8 \mapsto 7_8$, $7_8 \mapsto 3_8$

2) $1_8 \mapsto 1_8$, $3_8 \mapsto 7_8$, $5_8 \mapsto 3_8$, $7_8 \mapsto 5_8$

3) $1_8 \mapsto 1_8$, $3_8 \mapsto 3_8$, $5_8 \mapsto 7_8$, $7_8 \mapsto 5_8$

4) analogicky další

celkem jich je 6 (3!)

4 13-19:59

DĚLITELÉ NULY

DEF.: Dělitelé nuly v okruhu $(R, +, \cdot)$ jsou takové nenulové prvky $a, b \in R$, pro něž platí $a \cdot b = 0_R$ ← neutr. prvek k +

např. $\mathbb{Z}_8$ dělitelé nuly $[2]_8, [4]_8$

JAK SE TO HLEDÁ?

Mějme $a \neq 0_R$, chceme najít $b \in R$, $b \neq 0_R$, aby $a \cdot b = 0_R$.

$(\mathbb{Z}_{14}, +)$ $a \neq [0]_{14}$

$[a]_{14} \cdot [b]_{14} = [0]_{14}$

$[a]_{14} \cdot [b]_{14} = [14]_{14}$

$a \cdot b \mid 14 \cdot k$ hledám

$a \neq 0_R$ pak b je dělitelem 14.

74.5 $(R, \oplus, \odot)$ $R = \mathbb{Q}$

$a \oplus b = a + b + 1$

$a \odot b = a + b + ab$

Tím, že je okruh, chci dělitele nuly $(0_R = -1)$

mám $a \neq 0_R$ hledám b:

$a \odot b = 0_R$

$a + b + ab = -1$

$b(1+a) = -1 - a$

$b = \frac{-1-a}{1+a}$

$b = -\frac{1+a}{1+a} = \underline{\underline{-1}} = 0_R$

$\Rightarrow$ nemá dělitele 0_R.

Ještě těleso:

tj. každý nenulový prvek musí mít inverzi k násobení:

$a \in R$ pevné chci a^{-1} inverzi k $\odot$

$a \odot a^{-1} = 1_R$ $1_R = 0$

$a + a^{-1} + a \cdot a^{-1} = 0$

$a^{-1}(1+a) = -a$ $\boxed{a^{-1} = \frac{-a}{1+a}}$

4 13-20:33

VĚTA O DĚLENÍ SE ZBYTKEM PRO POLYNOMY:

$f, g \in R[x]$ nekonstantní, $g \neq 0$.

Pak $\exists$ polynomy $r(x)$, $q(x)$ tak, že

$$f(x) = q(x) \cdot g(x) + r(x)$$

kde $0 \leq \deg r(x) < \deg g(x)$

$(2x+4,\ 2x^2+2x+2) = 2$ → konstanta

nesoudělné polynomy

4 13-20:51

84. Kolik polynomů $f(x) \in \mathbb{Z}_5$ takových, že $f(3) = 2$; $\deg f(x) = 3$

$f: ax^3 + bx^2 + cx + d$

$f(3) = 2$

$2a - b + 3c + d = 2 \Rightarrow 2a = 2 + b - 3c - d$

$d = 1$ [_ , _ , _ , _]

$c = r$ a s r 1

$b = s$ $5 \cdot 5 \cdot 5 = 125$

stupeň nejvýše 3

polynomů st 0 0

st 1 ..... 1 $(x-1)$,

st 2 .....

Rychleji:

koef $a \neq 0$ .... 4 možnosti pro a

b, c ... volím ... $5 \cdot 5$

d ... dopočítám

$4 \cdot 5 \cdot 5 = 100$

4 13-20:57

METODA NEURČ. KOEFICIENTŮ

$(x - x_1)(x - x_2)(x - x_3)(x - x_4) =$

$= x^4 - 3x^3 + 5x^2 - 4x + 2 = f$

L: $(x^2 + (-x_1 - x_2)x + x_1 \cdot x_2)(x^2 + (-x_3 - x_4)x + x_3 x_4)$

$= x^4 + (-x_1 - x_2) \cdot x^3 + x_1 \cdot x_2 x^2 +$

$+ (-x_3 - x_4)x^3 + (-x_1 - x_2)(-x_3 - x_4)x^2 +$

$+ x_1 \cdot x_2(-x_3 - x_4)x + x_3 \cdot x_4 \cdot x^2 +$

$+ x_3 x_4(-x_1 - x_2)x + x_1 \cdot x_2 \cdot x_3 \cdot x_4$

může $f = (x^2 + ax + b)(x^2 + cx + d)$

4 13-21:11

63) 1) $\varphi: \mathbb{Z} \to \mathbb{Z}$

jediné podgrupy v $(\mathbb{Z}, +)$ jsou ve tvaru $n \cdot \mathbb{Z}$, kde $n \in \mathbb{N}$, a jedna $\{0\}$

Takže homomorfismů je tolik jako přir. čísel + 1 za nulový

4 13-21:21

64. 3 $\varphi: \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$

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

řády $\underline{1}$ $\underline{2}$ $\underline{2}$ $\underline{2}$

$Z = 0_4, 1_4, 2_4, 3_4$

řády 1, 4, 2, 4

$\mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4$

$(0, 0) \longmapsto [0]_4$ $[1_2, 1_2] \longrightarrow [0]_4$

$\left\{ \begin{array}{l} (0_2, 1_2) \longmapsto [2] \text{ } 0_4 \\ [1_2, 0_2] \longmapsto [2]_4 \end{array} \right.$

TRIVIÁLNÍ

1 ks

1 ks

2

4 13-21:26