Homomorfismy

$f : (X, +, 0, -) \to (Y, *, 1, ^{-1})$

$f(x_1 + x_2) = f(x_1) * f(x_2)$

$f(0) = 1$

$f(-x) = (f(x))^{-1}$

$\Rightarrow$ f HOMOMORFISMUS GRUP.

Tvrzení $(A, *, e_A, {}^{-1})$ $(B, \top, e_B, {}^{-1})$ grupy

$f: A \to B$ homomorfismus pologrup $(A, *)$, $(B, \top)$. Pak f je homomorfismus grup A, B.

Důkaz 1) $f(e_A) = e_B$

$f(e_A) = f(e_A * e_A) = f(e_A) \top f(e_A)$

Existuje $(f(e_A))^{-1}$.

$f(e_A) \top (f(e_A))^{-1} = f(e_A) \top f(e_A) \top (f(e_A))^{-1}$

$e_B = f(e_A) \top e_B = f(e_A)$

2) $f(x) \top f(x^{-1}) = f(x * x^{-1}) =$

$= f(e_A) = e_B$

$\Rightarrow f(x^{-1}) = (f(x))^{-1}$

Izomorfismus

Bijektivní homomorfismus pologrup (monoidů, grup) se nazývá IZOMORFISMUS pologrup (monoidů, grup).

Tvrzení $f: A \to B$ izomorfismus pologrup (monoidů, grup). Pak $f^{-1}: B \to A$ je také izomorfismus pologrup (monoidů, grup).

Důkaz f^{-1} je bijekce ✓

$f^{-1}: (B, *) \longrightarrow (A, +)$

$y_1, y_2 \in B$

$f^{-1}(y_1 * y_2) \stackrel{?}{=} f^{-1}(y_1) + f^{-1}(y_2)$

$f\left(f^{-1}(y_1 * y_2)\right) = y_1 * y_2$

$f\left(f^{-1}(y_1) + f^{-1}(y_2)\right) =$

$f(f^{-1}(y_1)) * f(f^{-1}(y_2)) = y_1 * y_2$

$f^{-1}(y_1 * y_2) = f^{-1}(y_1) + f^{-1}(y_2)$.

zbytek DÚ.

Příklad 1) $(X, *, e, ^{-1})$

$id_X : X \longrightarrow X$, $x \mapsto x$. je izomorfismus.

2) $(\mathbb{R}, +, 0, -)$

$(\mathbb{R}_+, \cdot, 1, ^{-1})$ grupy

$\exp : (\mathbb{R}, +, 0, -) \to (\mathbb{R}_+, \cdot, 1, ^{-1})$

$x \mapsto e^x$

exp je bijekce.

$\exp(x) \cdot \exp(y) = \exp(x+y)$

$e^x \cdot e^y = e^{x+y}$

$\Rightarrow$ exp je homomorfismus.

Pologrupy (monoidy, grupy),
mezi nimiž existuje izomorfismus,
se nazývají IZOMORFNÍ ($\cong$).

$A \cong B$.

Tvrzení A, B, C jsou pologrupy (monoidy, grupy). Pak:

1) $A \cong A$ (reflexivita)
2) $A \cong B \Rightarrow B \cong A$ (symetrie)
3) $A \cong B \wedge B \cong C \Rightarrow A \cong C$ (tranzitivita).

Důkaz. DÚ

Zbytkové třídy

$\mathbb{Z}$, $m \in \mathbb{N}$, $m > 1$

$\mathbb{Z}_m$

$[0]_m = \{\dots, -2m, -m, 0, m, 2m, \dots\}$

$[1]_m = \{\dots, -2m+1, -m+1, 1, m+1, 2m+1, \dots\}$

$\vdots$

$[m]_m = \{\dots, -2m, -m, 0, m, 2m, 3m, \dots\}$

dostáváme na třídě $[0]_m, [1]_m, \dots, [m-1]_m$, které tvoří $\mathbb{Z}_m$

$[a]_m + [b]_m = [a+b]_m$

$[0]_m$

$-[a]_m = [-a]_m$

$m = 3 \Rightarrow \mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$

$[1]_3 + [2]_3 = [1+2]_3 = [3]_3 = [0]_3$

$-[2]_3 = [1]_3$

OKRUHY A POLE

X množina s následujícími vlastnostmi:

1) na X máme binární operaci $+$,
2) na X máme binární operaci $\cdot$,
3) v X existují prvky $0, 1$ $(0 \neq 1)$,
4) máme zobrazení $X \to X$, $x \mapsto -x$,

takové, že

a) $x + (y+z) = (x+y)+z$,
b) $x+y = y+x$,
c) $x+0 = 0+x = x$,
d) $x+(-x) = (-x)+x = 0$,
e) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,
f) $x \cdot y = y \cdot x$,
g) $x \cdot 1 = 1 \cdot x = x$,
h) $x \cdot (y+z) = x \cdot y + x \cdot z$.

Potom X se nazývá OKRUH.

Okruh, ve kterém ke každému prvku různému od 0 existuje prvek inverzní vzhledem k operaci $\cdot$, se nazývá POLE.

Tvrzení Množina $\mathbb{Z}_m$, $m > 1$, zbytkových tříd modulo m tvoří pole právě tehdy, když m je prvočíslo.

Tvrzení P ... pole, $a, b \in P$.
Je-li $a \neq 0$, pak existuje jediný prvek $\xi \in P$ takový, že

$$a\xi + b = 0,$$

a sice prvek $\xi = -ba^{-1}$ a nazývá se ŘEŠENÍ rovnice $ax + b = 0$.

Důkaz $\xi = -b \cdot a^{-1}$

$$a\xi + b = a \cdot ((-b) \cdot a^{-1}) + b =$$
$$= (a \cdot a^{-1}) \cdot (-b) + b = 1 \cdot (-b) + b = 0.$$

$$a\xi + b = 0$$
$$a\xi = -b$$