Algr.

prednáška 12.3.2007

Grupy

Nech p je polynóm nad R s celočíselnými koeficientami

$p(x) = x^2 + 5x + 6 = (x+2)(x+3)$

$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ → vzorec pre riešenie pol. st. 2

∃ vzorec pre riešenie polynómov st. 3, 4

∄ vzorec pre riešenie stupňa 5 a viac?

Galois dokázal, že nie a okrem toho nemajú riešenia štyri problémy – kvadratúra kruhu
– trisekcia uhla

Grupa – je grupoid $(G, \cdot)$ s týmito vlastnostami

(asociativita) (G1)

Pre všetky $a, b, c \in G$ platí, že $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(existencia jednotky) – monoid

(G2) Existuje $e \in G$ také, že pre všetky $a \in G$ platí $a \cdot e = e \cdot a = a$

(G3): Existencia inverzného prvku

Pre každé $a \in G$ existuje $a^{-1} \in G$ také, že $a \cdot a^{-1} = e$ ← jednotkový prvok

Odcenuz: - namiesto „$(G, \cdot)$ je grupa" G je grupa

- namiesto $x \cdot y = xy$

Veta 1: nech G je grupa, $a \in G$, a^{-1} je inverzný k a (tj. $a\,a^{-1} = e$). Potom a je inverzný k a^{-1} (tj. $a^{-1} \cdot a = e$)

Dôkaz:

$a^{-1} = a^{-1} e = a^{-1}(a \cdot a^{-1}) = (a^{-1} \cdot a) \cdot a^{-1}$ ⇒ $a^{-1} = (a^{-1} a)\, a^{-1}$ (*)

G_3 G_2 G_1

Keďže $a^{-1} \in G$, má inverzný prvok v G $a^{-1} \cdot (a^{-1})^{-1} = e$

Vynásobme (* sprava prvkom $(a^{-1})^{-1}$

$a^{-1} \cdot (a^{-1})^{-1} = ((a^{-1} \cdot a) \cdot a^{-1})(a^{-1})^{-1}$

ale $a^{-1} \cdot (a^{-1})^{-1} = e$ (G_3) ⇒ $e = ((a^{-1} \cdot a) \cdot a^{-1})(a^{-1})^{-1}$

$e = (a^{-1} \cdot a) \cdot \underbrace{(a^{-1}) \cdot (a^{-1})^{-1}}_{e} = (a^{-1} \cdot a)\, e =$

$e = a^{-1} \cdot a$ □

Veta 2 (o krátení v grupe)

Nech G je grupa, nech $a, b, x \in G$ také, že

buď $x.a = x.b$ alebo $a.x = b.x$ (jedno stačí)

Potom $a = b$

Dôkaz Nech $x.a = x.b$. Potom $(x^{-1})x.a = (x^{-1}).x.b$

$e.a = e.b$

$a = b$

$a.x = b.x \Rightarrow a = b$ je dokázaná podobne

Veta 3: (o jednoznačnosti inverzného prvku)

Ak x_1 a x_2 sú inverzné k a, potom $x_1 = x_2$

Dôkaz $a.x_1 = e$

$a.x_2 = e$

$a.x_1 = a.x_2$; vykrátime a podľa vety 2

$x_1 = x_2$ □

Teda $\{(a, a^{-1}).\ a \in G\}$ je zobrazenie

$a \mapsto a^{-1}$ je zobrazenie

Veta 4 Nech G je grupa. Pre všetky $x \in G$

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

Dôkaz

$(x^{-1}).(x^{-1})^{-1} = e$ (G_3)

$(x^{-1}).x = e$ (Veta 1)

} krátenie x^{-1} $\quad x = (x^{-1})^{-1}$

Veta: Nech G je grupa, $a_1, \dots a_n \in G$

Potom $(a_1, \dots, a_n)^{-1} = a_n^{-1} \dots a_1^{-1}$

Dôkaz: $(a_1 \dots a_{n-1}.a_n).(a_n^{-1}.a_{n-1}^{-1} \dots a_1^{-1}) = (a_1 \dots a_{n-1})\underbrace{(a_n.a_n^{-1})}_{e}(a_{n-1}^{-1} \dots a_1^{-1}) =$

$= (a_1 \dots a_{n-1})(a_{n-1}^{-1} \dots a_1) = a_1 a_1^{-1} = e$

($n-1$ krokov)

$(a_1 \cdot \ldots \cdot a_{n+1})(a_n^{-1} \cdot \ldots \cdot a_1^{-1}) = e$

inverzný prvok k

□

Príklad $(\mathbb{R}, +)$

neutrálny prvok 0

k prvku $x \in \mathbb{R}$ je inverzný $(-x)$

$x^{-1} = -x$ grupový zápis

Príklad $(\mathbb{R}, \cdot)$

neutrálny prvok je 1

k prvku $x \in \mathbb{R}$ je inverzný $\frac{1}{x}$, neexistuje pre $x = 0$

0 nemá inverzný prvok, muselo by byť

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

a to nie je

nech by bolo 0^{-1} hocičo

$0 \cdot 0^{-1} = 0 \neq 1$

Príklad $(\mathbb{R} \setminus \{0\}, \cdot)$

- je operácia na $\mathbb{R} \setminus \{0\}$? áno

$x \neq 0, y \neq 0 \Rightarrow x \cdot y \neq 0$

asociativita $\cdot$? áno lebo $(\mathbb{R}, \cdot)$ je pologrupa

neutrálny prvok je 1

inverzný prvok k x je $\frac{1}{x}$

Príklad $(2^{\mathbb{N}}, \cup)$

(G1) platí $(A \cup B) \cup C = A \cup (B \cup C)$

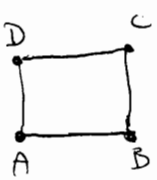
(G2) e neutrálny prvok: $\emptyset$

(G3) $\forall A \in 2^{\mathbb{N}} \; \exists A^{-1} \in 2^{\mathbb{N}} : A \cup A^{-1} = \emptyset$

neplatí: Ak $A = \{1\}$ $\{1\} \cup \{1\}^{-1} \ni 1 \Rightarrow \{1\} \cup \{1\}^{-1} \neq \emptyset$, nech už $\{1\}^{-1}$ hocičo

$(\mathbb{Z} \setminus \{0\}, \cdot)$ nie je grupa

Príklad



Symetrie (rovinné) sú také zobrazenia roviny do seba, ktoré zachovávajú vzdialenosť v ľubovoľných dvoch bodov

$f : \text{Rovina} \to \text{Rovina}$

$\forall A, B \in \text{Rovina} : |AB| = |f(A)f(B)|$

dĺžka úsečky

Príklady -id
- osová súmernosť
- stredová súmernosť
- posunutie
- otočenie

f, g symetrie $\Rightarrow$ $f \circ g$ je symetria

f^{-1} je inverzne zobrazenie (je tiež symetria)

(Symetrie, $\circ$)

$\downarrow$

Grupa

Symetria rovinného útvaru U je taká symetria roviny, ktorá zobrazí U do seba

Symetria štvorca

$\circ$	id	1	—	/	\	$\circlearrowright_{180}$
id	A B C D	B A D C	D C B A	A D C B	C B A D	C D A B
1	B A D C	A B C D	C D A B	D A B C	B C D A	A D C B
—	D C B A	C D A B	A B C D	B A D C	A D C B	B A D C
/	A D C B	D A B C	B C D A	A B C D	C D A B	B C D A
\	C B A D	B C D A	A D C B	C D A B	A B C D	D A B C
$\circlearrowright_{180}$	C D A B	B C D A	A D C B	C D A B	A B C D	D A B C

$\circ$	A	B	C	D
$\circlearrowright_{90}$	D	A	B	C
$\circlearrowright_{180}$	C	D	A	B
$\circlearrowright_{270}$	B	C	D	A

Zobrazenia (permutácie) na $\{A, B, C, D\}$

tvoria grupu so skladaním

Homomorfizmus grúp.

Definícia

Nech G, H sú grupy.

$\varphi: G \to H$ je homomorfizmus

práve vtedy, keď

pre všetky $a, b \in G$

$$\varphi(a, b) = \varphi(a) . \varphi(b)$$

$\in G$ $\in H$

Príklad: $G = \mathbb{R} \setminus \{0\}$, operácia $\cdot$.

$H = \mathbb{R}^+$, operácia $\cdot$.

$\varphi(x) = |x|$

$\varphi(a.b) = |a.b| = |a| . |b| = \varphi(a) . \varphi(b)$

Príklad: $G = \mathbb{R}$, operácia $+$

$H = \mathbb{R}^+$, operácia $\cdot$.

$\varphi : G \longrightarrow H$

$\varphi(a+b) = \varphi(a) . \varphi(b)$ $\qquad \varphi(a+b) = e^{a+b} = e^a . e^b = \varphi(a) . \varphi(b)$

$\varphi(x) = e^x$

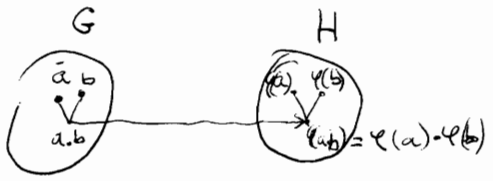
Príklad: $G = \mathbb{R}^+$, operácia $\cdot$.

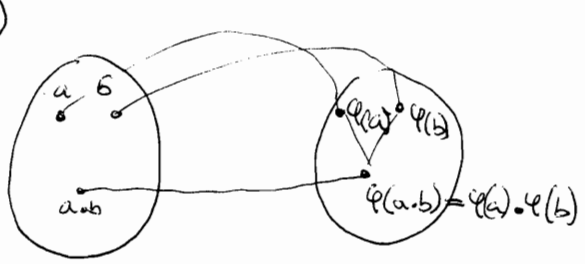
$H = \mathbb{R}$, operácia $+$

$\varphi : G \longrightarrow H$

$\varphi(x) = \ln x$

$\varphi(a.b) = \ln(a.b) = \ln(a) + \ln(b) = \varphi(a) + \varphi(b)$





Príklad

$G = \mathbb{R} \setminus \{0\}$, operácia $\cdot$.

$H = \{-1, 1\}$, operácia $\cdot$.

$\varphi : G \longrightarrow H$

$\varphi(x) = \dfrac{x}{|x|}$ $\qquad \varphi(a.b) = \dfrac{a.b}{|a.b|} = \dfrac{a.b}{|a| . |b|} = \dfrac{a}{|a|} . \dfrac{b}{|b|} = \varphi(a) . \varphi(b)$