Algebraické štruktúry

March 11, 2020

Definícia

Nech $(G, *)$ je pologrupa. Ak

1. v $(G, *)$ existuje neutrálny prvok e,
2. $\forall a \in G \, \exists a' \in G$ s vlastnosťou, že $a * a' = a' * a = e$,

potom $(G, *)$ sa nazýva grupa.

Grupa je teda monoid uzavretý na inverzné prvky.

Príklady grúp:

- $(\mathbb{Z}, +)$
- $(R, +)$
- $(R \setminus \{0\}, \cdot)$

Veta o krátení v grupe

Nech $(G, *)$ je grupa. Potom $a * b = a * c$ implikuje že $b = c$.
Analogicky $b * a = c * a$ implikuje $b = c$.

Dôkaz.
Nech $a, b, c \in G$ a $a * b = a * c$. Pretože $a' \in D$, tak $a' * (a * b) = a' * (a * c)$ a platí asociatívny zákon, tak $(a' * a) * b = (a' * a) * c$. Pretože $a * a' = e$, tak potom $b = c$.

Napríklad $(R, \cdot)$ nie je grupa. Neplatí zákon o krátení:
$0 \cdot 2 = 0 \cdot 3$ neimplikuje $2 = 3$.

Veta

Nech dvojica $(G, *)$ je pologrupa. $(G, *)$ je grupa práve vtedy ak $\forall a, b \in G$ existuje jednoznačné riešenie rovníc:

$$a * x = b \quad a \quad y * a = b.$$

Lema (Veta o krátení 2.)

Nech $(G, *)$ je pologrupa a $\forall a, b \in G$ existuje jednoznačné riešenie rovníc:

$$a * x = b \quad a \quad y * a = b.$$

Potom $a * b = a * c$ implikuje že $b = c$, a analogicky $b * a = c * a$ implikuje $b = c$

Dôkaz.
Nech $a, y \in G$ Potom $\exists! b \in G$ s vlatnosťou, že $a * b = y$. Teda $y = a * b = a * c$, potom $b = c$.

Dôkaz.

"$\Rightarrow$"
Nech $(G, *)$ je grupa a $a, b \in G$. Potom

$$\begin{aligned} a * x &= b \\ a' * (a * x) &= a' * b \\ (a' * a) * x &= a' * b \\ x &= a' * b. \end{aligned}$$

Teda vždy existuje riešenie $x = a' * b$.
Ak by existovali dve riešenia x_1 a x_2, potom z vety o krátení dostaneme $x_1 = x_2$.
Analogicky rovnica $y * a = b$ má jediné riešenie $y = b * a'$.

"$\Leftarrow$"

Nech $(G, *)$ je pologrupa a $\forall a, b \in G$ existuje jednoznačné riešenie rovníc:

$$a * x = b \quad a \quad y * a = b.$$

Ukážeme, že $(G, *)$ je grupa. Potrebujeme teda ukázať, že existuje neutrálny prvok e a ku každému $a \in G$ existuje inverzný prvok a'.
Z predpokladu vieme, že existujú jednoznačné riešenia rovníc:

$$a * x = a, \qquad y * a = a.$$

Označme riešenia: $x = a_P$ a $y = a_L$. Potom platí:

$$\begin{aligned} a * a &= (a * a_P) * a \\ &= a * (a_P * a) \\ a &= a_P * a. \end{aligned}$$

Pretože

$$a_L * a = a = a_P * a,$$

tak z Lemmy vyplýva, že

$$a_L = a_P = e_a$$

a teda

$$e_a * a = a * e_a = a.$$

Nech $b \in M$, $b \neq a$ a $e_b * b = b$. Potom platí

$$\begin{aligned} a * b &= (a * e_a) * b \\ a * (e_b * b) &= a * (e_a * b) \\ e_b * b &= e_a * b \\ e_b &= e_a \end{aligned}$$

To znamená, že existuje neutrálny prvok $e = e_a$, pre každé $\in G$.

Teraz ukážeme, že $\forall a \in M\ \exists a' \in M$ s vlastnosťou

$$a * a' = a' * a = e.$$

Vieme, že rovnica $a * x = e$ má jediné riešenie. Označme ho a'_P . Analogicky a'_L označíme riešenie rovnice $y * a = e$.

$$\begin{aligned} a * a'_P &= e \\ (a * a'_P) * a &= e * a = a = a * e \\ a * (a'_P * a) &= a * e \end{aligned}$$

Z Lemy dostaneme $a'_P * a = e$. Pretože $a'_L * a = a'_P * a$, tak $a'_P = a'_L$ Označme riešenie rovníc a'. a' je inverzný prvok k prvku a. To znamená, že $(G, *)$ je grupa.

Tvrdenie

Nech $(M, *)$ je grupa, potom:

(a) $(a')' = a$, pre $\forall a \in M$;

(b) $(a * b)' = b' * a'$, pre $\forall a, b \in M$;

(c) $(a * b)' = a' * b'$ práve vtedy ak $a * b = b * a$.

Dôkaz.

(a) Pretože $a' \in M$, tak $(a')' \in M$ a naviac platí $(a')' * a' = e$. Teda

$$((a')' * a') * a = e * a$$

$$(a')' * (a' * a) = a$$

$$(a')' = a.$$

(b) Ak $a * b \in M$, potom $(a * b)' \in M$ a platí

$$\begin{aligned}
(a * b)' * (a * b) &= e \\
((a * b)' * a) * b &= e \\
((a * b)' * a) * b * b' &= e * b' \\
(a * b)' * a &= b' \\
(a * b)' * a * a' &= b' * a' \\
(a * b)' &= b' * a'.
\end{aligned}$$

(c) Ak $a * b = b * a$, potom $(a * b)' = (b * a)'$ a teda

$$a' * b' = b' * a'.$$

Teraz ukážeme opačnú implikáciu. Nech $a' * b' = b' * a'$, potom

$$\begin{aligned}
a * (a' * b') &= a * (b' * a') \\
b' &= (a * b') * a' \\
b' * a &= ((a * b') * a') * a \\
b' * a &= a * b' \\
b * (b' * a) &= b * (a * b') \\
a &= (b * a) * b' \\
a * b &= (b * a) * b' * b \\
a * b &= b * a.
\end{aligned}$$

Poznámka

Vidíme, že

- $((a * b) * c)' = c' * b' * a'$, pre $\forall a, b, c \in M$;
- ak označíme $a * a = a^2$ a $a^k = a^{k-1} * a$, pre $k \in I$, potom $a^1 = a$, $a^0 = e$, $a^{-1} = a'$ a $a^{-k} = (a^k)^{-1} = (a^{-1})^k$ a navyše $a^{k+n} = a^k * a^n$;

Definícia

Nech $(M, *)$ je grupa a pre $\forall a, b \in M$ $a * b = b * a$ potom dvojica $(M, *)$ sa nazýva *Abelova grupa*.

Príklady:
1) Nech $p \in N$. Dokážte, že
a) $(Z_p, +)$ je Abelova grupa pre každé p;
b) $(Z_p \setminus \{0\}, \cdot)$ je grupa práve vtedy, ak p je prvočíslo.
2) Zistite či $((Z_5 \setminus \{0\})^2, \circ)$ je Abelova grupa, ak $(a, b) \circ (c, d) = (a \cdot c, b \cdot d)$ pre $a, b, c, d \in Z_5 \setminus \{0\}$.
3) Zistite či $(Z_5^2, \circ)$ je Abelova grupa, ak $(a, b) \circ (c, d) = (a \cdot c, b \cdot d)$ pre $a, b, c, d \in Z_5$.
4) Nech $M = \{[t, s];\ t, s \in R^1)$ a $[t_1, s_1] \oplus [t_2, s_2] = [t_1 + t_2, s_1 + s_2]$. Zistite či $(M, \oplus)$ je Abelova grupa.
5) Nech $M = \{[t, s];\ t, s \in \{x \in R^1;\ x > 0\})$ a $[t_1, s_1] \circ [t_2, s_2] = [t_1 \cdot t_2, s_1 \cdot s_2]$. Zistite či $(M, \circ)$ je Abelova grupa.
6) Nech M je množina všetkých matíc 2×2, prvky matice sú reálne čísla a $A + B$, $A \cdot B$ sú obvyklé operácie súčtu a násobenia matíc. Zistite či $(M, +)$ a $(M, \cdot)$ sú grupy.

Definícia

Nech $(G_1, \circ)$ a $(G, *)$ sú grupy. Ak $G_1 \subseteq G$ a $\forall a, b \in G_1 \; a \circ b = a * b$ ($\circ = *$ na G_1), potom grupa $(G_1, *)$ sa nazýva podgrupa grupy $(G, *)$.

Príklad

Máme grupu $(Z_{12}, \oplus_{12})$, kde operácia $\oplus_{12}$ je štandarná binárna operácia na zvyškovej triede rádu 12. Nech $G_1 = \{0, 6\}$ a $M = \{0, 1, 2\}$.

- Dvojica $(G_1, \oplus_{12})$ je grupa a teda je podgrupa $(Z_{12}, \oplus_{12})$.
- Množina $M \subseteq Z_{12}$ a $(M, \oplus_3)$ je grupa, ale $\oplus_3 \neq \oplus_{12}$. Dvojica $(M, \oplus_{12})$ nie je ani grupoid. Napríklad $2 \oplus_{12} 2 = 4 \notin M$.

$\oplus_{12}$	0	1	2
0	0	1	2
1	1	2	$\times$
2	2	$\times$	$\times$

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table: $(M, \oplus_{12})$ nie je grupoid a $(M, \oplus_3)$ je abelova grupa

Tvrdenie

Nech $(G, *)$ je grupa a $M \subseteq G$. $(M, *)$ je podgrupa grupy $(G, *)$ ak platia nasledujúce vlastnosti:

a) $(M, *)$ je grupoid (množina M je uzavretá vzhľadiom na operáciu $*$.)

b) $\forall x \in M\ x' \in M$.

Dôkaz.
Stačí ukázať, že neutrálny prvok patrí do M. Pretože $x \in M$ implikuje $x' \in M$ a z vlastnosti a) dostaneme

$$a * a' = e \in M.t$$

Tvrdenie

Nech $(G, *)$ je grupa a $M \subseteq G$. Ak $(M, *)$ je podgrupa grupy $(G, *)$ práve vtedy ak $\forall x, y \in M\ x * y' \in M$.

Dôkaz.
"$\Rightarrow$"
Tvrdenie, že ak $(M, *)$ je podgrupa grupy $(G, *)$, potom $\forall x, y \in M\ x * y' \in M$, vypl'yva priamo z definície podgrupy.

Uvažujme grupu $(Z_{12}, \oplus_{12})$ a $S = \{2, 4, 6\}$

Chceme nájst všetky podgrupy $(G, \oplus_{12})$ grupy $(Z_{12}, \oplus_{12})$, pre ktoré platí $S \subseteq G$.

G musí byť uzavretá vzhľadom na operáciu $\oplus_{12}$ a ku každému prvku musí existovať inverzný. ľahko si overíme, že existujú dve také podgrupy: $G = \{2, 4, 6, 8, 10, 0\}$ a $G = Z_{12}$.

Teda $(G, \oplus_{12})$ a $(Z_{12}, \oplus_{12})$.

Pretože $G \subseteq Z_{12}$, tak G je najmenšia taká podgrupa. Množina S generuje grupu $(G, \oplus_{12})$.

Nech $(G, *)$ je grupa. Označme $a^2 = a * a$. Je zrejme, že $a * a * a = (a * a) * a = a^2 * a$. Z asociativity operácie $*$ vyplýva, že $a * a^2 = a^2 * a = a^3$.
Ak povieme, že grupa je aditívna, tak binárnu operáciu "$*$" označujeme "$+$", t.z. $a * b = a + b$, neutrálny prvok $e = 0$ a inverzný prvok k prvku a zapíšeme ako $-a$ ($a' = -a$).

Definícia

Nech $(G, *)$ je grupa a $k \in Z$ a $x \in G$.
a) položme $x^1 = x$ a $x^k = x^{k-1} * x$ (multiplikatívna grupa);
b) položme $1 \times x = x$ a $k \times x = kx = (k-1)x * x$ (aditívna grupa);

Tvrdenie

Nech $(G, *)$ je grupa. Potom $\forall x \in G$ a $\forall n, k \in Z$ platí:

(i) $x^0 = e$;

(ii) $x^{-k} = (x')^k$;

(iii) $x^{k+n} = x^k * x^n$;

(iv) $\left(x^k\right)^n = x^{kn}$.

Dôkaz.

(i)

$$e * x = x = x^1 = x^{1-1} * x = x^0 * x.$$

Teda

$$e * x = x^0 * x \qquad \Rightarrow \qquad e = x^0.$$

(ii)

$$x' * x = e = x^0 = x^{0-1} * x = x^{-1} * x.$$

Teda

$$x' * x = x^{-1} * x \qquad \Rightarrow \qquad x' = x^{-1}.$$

(iii) a (iv) zrejmé.

Ak grupu $(M, *)$ nazveme aditívnou, potom píšeme $(M, +)$ a platí:

1. $a = (a^{-1})^{-1} = -(-a)$ a $a * b^{-1} = a - b$;
2. $(a * b)^{-1} = -(a + b) = -b - a$;
3. $((a * b) * c)^{-1} = -c - (a + b) = -c - b - a$;
4. $a * a = (a^2)_* = a + a = 2a$ a $(a^0)_* = 0$,

$$(a^k)_* = a^{k-1} * a = \left(\sum_i^{k-1} a\right) + a = (k-1)a + a,$$

$$(k-1)a = \underbrace{a + a + \cdots + a}_{(k-1)- \text{ krát}}$$

pre $k \in N$.

5. Ak $a + b = b + a$, potom

$$a - (a - b) = a + \left(a + b^{-1}\right)^{-1} = \left(a + a^{-1}\right) + b = 0 + b = b.$$

V prípade multiplikatívnej grupy sa používa symbol násobenia reálnych čísel, t.z. $a * b = ab = a \cdot b$ a neutrálny prvok označíme 1 ($e = 1$). Ak grupu $(M, *)$ nazveme multiplikatívnou, potom píšeme $(M, \cdot)$ a

1. $a = (a^{-1})^{-1}$;
2. $(a * b)^{-1} = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = b^{-1}a^{-1}$;
3. $((a * b) * c)^{-1} = c^{-1} \cdot b^{-1} \cdot a^{-1}$;
4. $a * a = a \cdot a = a^2$ a $a^0 = 1$;