Algebraické štruktúry

1 Grupa

Definícia 1 *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.*

Poznámka 1 *Grupa je teda monoid uzavretý na inverné prvky.*

Tvrdenie 1 *(Veta o krátení) Nech* $(G, *)$ *je pologrupa a* $\forall a, b \in G$ *existuje jednoznačné riešenie rovníc:*

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

Potom z rovnosti $a * b = a * c$ $(b * a = c * a)$ *vyplýva, že* $b = c$*.*

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

Tvrdenie 2 *Nech dvojica* $(G, *)$ *je pologrupa.* $(G, *)$ *je grupa práve vtedy ak* $\forall a, b \in G$ *existuje jednoznačné riešenie rovníc:*

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

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

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

Teda vždy existuje jediné $x = a' * b$. 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 Tvrdenia 1 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 rovnice

$$a * x = e = y * a$$

majú jediné riešenie a $y = y * e$. Potom

$$y = y * (a * x) = (y * a) * x = e * x = x.$$

Označme riešenie rovníc a'. Teda $a * a' = a' * a = e$. To znamená, že $(G, *)$ je grupa.

■

Tvrdenie 3 *Nech $(M, *)$ je grupa, potom:*

1. $(a')' = a$, *pre* $\forall a \in M$;
2. $(a * b)' = b' * a'$, *pre* $\forall a, b \in M$;
3. $(a * b)' = a' * b'$ *práve vtedy ak* $a * b = b * a$.

Dôkaz.

1. Pretože $a' \in M$, tak $(a')' \in M$ a naviac platí

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

Teda

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

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

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

3. 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

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

Poznámka 2 *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 2 *Nech* $(M, *)$ *je grupa a pre* $\forall a, b \in M$ $a * b = b * a$ *potom dvojica* $(M, *)$ *sa nazýva* Abelova grupa.

Cvičenie 1 *Nech* $p \in N$. *Dokážte, že*
a) $(Z_p, +)$ *je Abelova grupa pre každé* p;
b) $(Z_p \backslash \{0\}, \cdot)$ *je grupa práve vtedy, ak* p *je prvočíslo.*

Cvičenie 2 *Zistite či* $((Z_5\backslash\{0\})^2, \circ)$ *je Abelova grupa, ak* $(a,b)\circ(c,d) = (a\cdot c, b\cdot d)$ *pre* $a,b,c,d \in Z_5\backslash\{0\}$.

Cvičenie 3 *Zistite či* $(Z_5^2, \circ)$ *je Abelova grupa, ak* $(a,b)\circ(c,d) = (a\cdot c, b\cdot d)$ *pre* $a,b,c,d \in Z_5$.

Cvičenie 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.*

Cvičenie 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.*

Cvičenie 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.*

1.1 Podgrupy

Definícia 3 *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 1 *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	×
2	2	×	×

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

Table 1: $(M, \oplus_{12})$ nie je grupoid a $(M, \oplus_3)$ je abelova grupa

Tvrdenie 4 *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*

$$a * a' = e \in M. \qquad \blacksquare$$

Tvrdenie 5 *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.*

"$\Leftarrow$"
(i) Pre $\forall a \in M \; a * a' \in M$*. Teda* $e \in M$*.*
(ii) Ak $a \in M$*, potom* $e, a \in M$ *a teda* $e * a' = a' \in M$*. To znamená, že* $\forall a \in M \; a' \in M$*.*
(iii) Pre $\forall a, b \in M$ *z (ii) vyplýva, že* $a, b' \in M$ *a teda* $a * (b')' = a * b \in M$*.*
$\blacksquare$

Príklad 2 *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* $(G, \oplus_{12})$*.*

1.2 Kalkulus na grupách

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 4 *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 6 *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 $a^0 = 1$;

1.3 Cyklická grupa a podgrupa

Definícia 5 *Nech* $(G, *)$ *je grupa. Nech* $a \in G$. *Ak existuje* $n \in N$ *s vlastnosťou, že* $a^n = e$, *potom najmenšie tak číslo* n *nazývame rádom prvku* a *a píšeme* $r(a) = n$. *Ak také číslo neexistuje, povieme, že prvok má nekonečný rád.*

Poznámka 3 *Nie každá grupa nekonečným počtom prvkov je cyklická. Napríklad* $(R, +)$.

Definícia 6 *Nech* $(G, *)$ *je grupa. Ak existuje prvok* $a \in G$ *s vlastnosťou, že* $G = \{a^k;\ k \in Z\}$, *tak grupa* $(G, *)$ *sa nazýva cyklická grupa s generátorom* a *(*$G =< a >$*). Najmenšie také* k *nazývame rád grupy* G *(*$r(G) = k$*).*

Tvrdenie 7 *Každá cyklická grupa je komutatívna.*

Dôkaz.
Ak $< a >= G$, *tak* $\forall x, y \in G$ *existujú* $u, v \in Z$ *s vlastnosťou, že* $x = a^u$ *a* $y = a^v$. *Teda*

$$x * y = a^u * a^v = a^{u+v} = a^{v+u} = a^v * a^u = y * x.$$

∎

Cyklické grupy s nekonečným rádom

Tvrdenie 8 *Ak rád cyklickej grupy je* ∞, *potom pre* $\forall x \in G \backslash \{e\}$ *platí, že* $|x| = \infty$.

Dôkaz.
Nech G je nekonečná cyklická grupa generovaná prvkom a, To znamená. že $G = \{a^n; n \in Z\}$. *Ak* $x \in G$ *a* $x \neq e$, *potom* $x = a^u$ *pre nejaké* $u \neq 0$. *Ak* $k \in Z$, *potom*

$$x^k = (a^u)^k = a^{uk}.$$

Pretože $|a| = \infty$, *tak* $a^n = e$ *práve vtedy, ak* $n = 0$.
Nech $k \neq 0$ *a* $x^k = e$. *Potom*

$$x^k = a^{uk} = e = a^0 \qquad \Leftrightarrow \qquad uk = 0.$$

To znamená, že $k = 0$, *alebo* $u = 0$. *Čo je spor s predpokladom, že* $u \neq 0$ *a* $k \neq 0$. *Teda* $|x| = \infty$. ∎

Tvrdenie 9 *Nech G je cyklická grupa nekonečného rádu. Ak* $x \in G$ *a* $x \neq e$, *potom pre* $u, v \in Z$ *platí, že* $x^u = x^v$ *práve vtedy, ak* $u = v$.

Dôkaz.
"$\Rightarrow$"
Ak $a^u = a^v$, *tak*

$$a^u * a^{-v} = a^{u-v} = e = a^0.$$

a z predchádzajúceho Tvrdenia 8 dostaneme

$$a^{u-v} = e = a^0$$

práve vtedy, ak $u - v = 0$ *a teda* $u = v$.
"$\Leftarrow$" *Ak* $u = v$ *tak je zrejme, že* $a^u = a^v$. ∎

Príklad 3 *Uvedieme niekoľko príkladov cyklických grúp s nekonečným rádom.*

- $(Z, +)$ *jej generátor je napríklad* 1. *To znamená, že* $< 1 >= Z$.
- *Ak* $M = \{k \cdot 3;\, k \in Z\}$, *tak* $(M, +)$ *je cyklická grupa, jej generátor je napríklad* 3. *To znamená* $< 3 >= M$. *Je to podgrupa* $(Z, +)$.
- *Ak* $H = \{2^k,\, k \in Z\}$, *potom* $(H, \cdot)$, *kde binárna operácia* $\cdot$ *je klasická operácia násobenia, je cyklická grupa s generátorom* 2.

Všimnime si, že $(Z, +)$, $(M, +)$ *a* $(H, \cdot)$ *sú navzájom izomorfné.*

Cyklické grupy s konečným rádom

Poznámka 4 *Nie každá grupa konečným počtom prvkov je cyklická.*

Príklad 4 *Nech* $M = \{1, 5, 7, 11\}$, *potom* $(M, \circ_{12})$ *je abelova grupa, kde binárna operácia* $\circ_{12}$ *je klasická operácia násobenia modulo* 12. *To znamená, že napríklad*

$$5 \circ_{12} 7 = 2 \cdot 12 + 11 = 11 \qquad mod(12).$$

$$\begin{aligned} < 1 > &= \{1\}, \quad |1| = 1 \\ < 5 > &= \{1, 5\}, \quad |5| = 2 \\ < 7 > &= \{1, 7\}, \quad |7| = 2 \\ < 11 > &= \{1, 11\}, \quad |11| = 2 \end{aligned}$$

Vidíme, že $(M, \circ_{12})$ *nie je cyklická grupa.*

Príklad 5 *Nech* $H = \{1, 3, 7, 9\}$, *potom* $(H, \circ_{10})$ *je abelova grupa, kde binárna operácia* $\circ_{10}$ *je klasická operácia násobenia modulo* 10. *To znamená, že napríklad*

$$3 \circ_{10} 7 = 2 \cdot 20 + 1 = 1 \qquad mod(10).$$

$$\begin{aligned} < 1 > &= \{1\}, \quad |1| = 1 \\ < 3 > &= \{1, 3, 9, 7\}, \quad |3| = 4 \\ < 7 > &= \{1, 7, 9, 3\}, \quad |7| = 4 \\ < 9 > &= \{1, 9\}, \quad |9| = 2 \end{aligned}$$

Vidíme, že $(H, \circ_{10})$ *je cyklická grupa, ktorá má rád* 4. *Jej generátory sú* 3 *a* 7.

Tvrdenie 10 *Nech* $(G, *)$ *je cyklická grupa konečného rádu. Ak* $a \in G$ *a* $|a| = n$, *tak pre* $u, v \in Z$ *platí*

$$a^u = a^v \qquad \Leftrightarrow \qquad n|(u-v),$$

kde $n|(u-v)$ *znamená, že* n *delí* $u - v$.

Dôkaz.
Nech $a^u = a^v$. *Potom* $a^{u-v} = e = a^{kn}$, *kde* $k \in Z$. *Pretože* $u - v \in Z$, *tak* $u - v = gn + r$, *kde* $g, n, r \in Z$ *a* $0 \leqslant r < n$. *Teda*

$$e = a^{u-v} = a^{gn+r} = a^{gn} * a^r = e * a^r = a^r.$$

Pretože $r < n$, *tak* $r = 0$. *(Pripomíname, že* n *je najmenšie take prirodzené číslo, pre ktoré platí* $a^n = e$.*) Z toho vyplýva, že* $u - v = gn$ *a teda* $n|(u-v)$.
∎

Príklad 6 *Máme grupu* $(Z_6, \oplus_6)$. *Napríklad*

$$4 = 100 \cdot 6 + 4 = 20 \cdot 6 + 4 \qquad mod(6).$$

Teda

$$u = 604, v = 124 \;\Rightarrow\; u - v = 480.$$
$$\frac{480}{6} = 8 \qquad \Rightarrow \qquad 6|(604 - 124).$$

Tvrdenie 11 *Nech* $(G, *)$ *je grupa a prvok* $a \in G$. *Ak existuje* $k \in N$, *že* $a^k = e$, *tak* $G_k(a) = \{a^i;\ i = 1, 2, \cdots, k\}$ *je cyklická podgrupa grupy* G.

Dôkaz.
Vyplýva to priamo z definície cyklickej grupy. ∎

Tvrdenie 12 *Každá podgrupa cyklickej grupy je cyklická grupa.*

Dôkaz.
Nech $(H, *)$ *je podgrupa grupy* $(G, *)$. *Ak* G *je cyklická grupa* $a < a >= G$, *potom pre každé* $x, y \in H$ *existujú* $u, v \in Z$ *s vlatnosťou* $x = a^u$ *a* $y = a^v$. *Pretože* $x * y \in H$, *tak* $x * y = a^u * a^v = a^{u+v}$.

Cvičenie 7 *Nájdite všetký cyklické podgrupy grupy* $(M, *)$ *ak*
a) $(M, *) = (Z_5, +)$*;*
b) $(M, *) = (Z_5 \backslash \{0\}, .)$*;*
c) $(M, *) = (Z_6, +)$*;*
d) $(M, *) = (Z_7 \backslash \{0\}, .)$*;*
e) $(M, *) = (Z_8, +)$*.*

Riešenie Cv. 7.

a) Majme $(Z_5, +)$*. Potom*

$$\begin{aligned} M(0) =& \{0\}, \\ M(1) =& Z_5, \\ M(2) =& \{2, 4, 6, 8, 10, \dots\} = \{2, 4, 1, 3, 0\} \ [5], \\ M(3) =& \{3, 6, 9, 12, 15, \dots\} = \{3, 1, 4, 2, 0\} \ [5], \\ M(4) =& \{4, 8, 12, 16, 20, \dots\} = \{4, 3, 2, 1, 0\} \ [5]. \end{aligned}$$

Vidíme, že ak $a \in Z_5 \backslash \{0\}$*, potom* $M(a) = Z_5$*.*

b) Pretože $Z_5 \backslash \{0\} = \{1, 2, 3, 4\}$*, tak*

$$\begin{aligned} M(1) =& \{1\}, \\ M(2) =& \{2, 2^2, 2^3, 2^4, \cdots\} = \{2, 4, 3, 1\} \ [5], \\ M(3) =& \{3, 9, 27, 81, 243, \cdots\} = \{3, 4, 2, 1\} \ [5], \\ M(4) =& \{4, 16, 64, 256, \cdots\} = \{4, 1\} \ [5]. \end{aligned}$$

c) Majme $(Z_6, +)$*, teda* $Z_6 = \{0, 1, 2, 3, 4, 5\}$*, tak*

$$\begin{aligned} M(0) =& \{0\}, \\ M(1) =& \{0, 1, 2, 3, 4, 5\}, \\ M(2) =& \{2, (2+2), (4+2), \cdots\} = \{2, 4, 0\} \ [6], \\ M(3) =& \{3, 6, 9, \cdots\} = \{3, 0\} \ [6], \\ M(4) =& \{4, 8, 12, 16, \cdots\} = \{4, 2, 0\} \ [6], \\ M(5) =& \{5, 10, 15, 20, 25, 30, 35, \cdots\} = \{5, 4, 3, 2, 1, 0\} \ [6]. \end{aligned}$$

d) Majme $(Z_7\backslash\{0\}, .)$. *Potom*

$$\begin{aligned}
M(1) =&\{1\},\\
M(2) =&\{2, 2^2, 2^3, 2^4, \cdots\} = \{2, 4, 1\}\ [7],\\
M(3) =&\{3, 9, 27, 81, 243, \cdots\} = \{3, 2, 6, 4, 5, 1\}\}\ [7],\\
M(4) =&\{4, 16, 64, 256, \cdots\} = \{4, 2, 1, \}\}\ [7],\\
M(5) =&\{5, 5^2, 5^3, 5^4, \cdots\} = \{5, 4, , , , \}\}\ [7],\\
M(6) =&\{6, 6^2, 6^3, 6^4, \cdots\} = \{6, 1, , , , \}\}\ [7].
\end{aligned}$$

e) $(Z_8, +)$

$$\begin{aligned}
M(0) =&\{0\},\\
M(1) =&Z_8,\\
M(2) =&\{2, 4, 6, 0\},\\
M(3) =&\{3, 6, 9, 12, 15, 18, 21, 24, \cdots\} = \{3, 6, 1, 4, 7, 2, 5, 0\}\ [8],\\
M(4) =&\{4, 8, 12, \cdots\} = \{4, 0\}\ [8],\\
M(5) =&\{5, 10, 15, 20, 25, 30, 35, 40, \cdots\} = \{5, 2, 7, 4, 1, 6, 3, 0\}\ [8],\\
M(6) =&\{6, 12, 18, 24, 30, 36, 42, \cdots\} = \{6, 4, 2, 0\}\ [8],\\
M(7) =&\{7, 14, 21, 28, 35, 42, 49, 56, \cdots\} = \{7, 6, 5, 4, 3, 2, 1, 0\}\ [8].
\end{aligned}$$

1.4 Lagrangeova veta a jej dôsledky

ešte doplním, počet prvkov grupy, podgrupy,...

1.5 Symetrické grupy, permutácie (18.3.2019)

Cvičenie 8 *Máme odbĺžnik* D_2 *s vrcholmi* $A, B, C.D$. *Bijekcie (symetrické zobrazenia)* $f_i : D_2 \to D_2$*:*

- f_0 – *všetko nechá na mieste.*
- f_1 – *osová súmernosť horizontálne.*
- f_2 – *osová súmernosť vertikálne.*
- f_3 – *súmernosť podľa stredu.*

$$I = f_0 = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad f_1 = \begin{pmatrix} C & D \\ A & B \end{pmatrix}, \quad f_2 = \begin{pmatrix} B & A \\ D & C \end{pmatrix}, \quad f_3 = \begin{pmatrix} D & C \\ B & A \end{pmatrix} \tag{1}$$

Všimnime si, že pre každú f_i platí: $f_i \circ f_i = f_i^2 = f_0$. Na množine zobrazení $D_2 = \{f_0, f_1, f_2, f_3\}$ je binárna operácia skladania $\circ$ uzavretá:

$\circ$	I	f_1	f_2	f_3
I	I	f_1	f_2	f_3
f_1	f_1	I	f_3	f_2
f_2	f_2	f_3	I	f_1
f_3	f_3	f_2	f_1	I

Table 2: Calyeho tabuľka pre binárnu operáciu $\circ$.

Napríklad $f_2 \circ f_3$. Podľa (1):

$$f_2 = \begin{pmatrix} B & A \\ & \\ D & C \end{pmatrix}, \quad f_2 \circ f_3 = \begin{pmatrix} C & D \\ & \\ A & B \end{pmatrix} = f_1.$$

Vskutočnosti ak $i, j, k \in \{1, 2, 3\}$ a $k \neq i, j$, potom

$$f_i \circ f_j = \begin{cases} I, & i = j \\ & \\ f_k, & i \neq j \end{cases}$$

Teda $(D_2, \circ)$ je necyklická grupa s neutrálnym prvkom I.

Poznámka 5 *Nech $(G, *)$ je štvor-prvková grupa ($|G| = 4$). Potom sú len dve možnosti buď je cyklická, alebo nie je cyklická.*
Ak je cyklická, tak je izomorfná s $(Z_4, \oplus)$.
Ak nie je cyklická, potom každý jej prvok rôzny od neutrálneho prvku e ($r(e) = 1$) musí byť rádu 2. To znamená, že ak $G = \{e, a, b, c\}$, tak $a^2 = b^2 = c^2 = e$. Otázkou je, čomu sa rovná $a * b$. Je jasné, že $a * b \in \{e, a, b, c\}$. Ak

$$a * b = e \quad \Rightarrow \quad a * b = a * a \quad \Rightarrow \quad a = b; \tag{2}$$
$$a * b = a \quad \Rightarrow \quad a * b = a * e \quad \Rightarrow \quad b = e; \tag{3}$$
$$a * b = b \quad \Rightarrow \quad a * b = e * b \quad \Rightarrow \quad a = e; \tag{4}$$

Všetky tri prípady (2)–(4) sú sporom s predpokladom, teda zostáva jediná možnosť $a * b = c$. Analogicky by sme ukázali, že $b * a = c$. Teda ak štvorprvková grupa $(G, *)$ nie je cyklická, potom je izomorfná s abelovou grupou, ktorá je daná nasledujúcou Caleyho tabuľkou 3:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 3: Calyeho tabuľka pre binárnu operáciu $*$.

Z toho vyplýva, že štvorprvková grupa je vždy abelova.

Definícia 7 *Nech A je konečná množina. Potom každá usporiadaná n-tica pozostávajúca z navzájom rôznych prvkov množiny A sa nazýva* permutácia.

Poznámka 6 *Nech $|A| = n$, $n > 0$. Koľko n-tíc môžeme zostaviť z prvkov množiny A, ak každý prvok smieme použiť práve raz? Máme teda n-prázdnych políčok, na ktoré budeme postupne umiestňovať prvky z množiny A. Hľadáme všetky permutácie $(x_1, x_2, \ldots, x_n)$, kde $x_i \in A$ a pre $\forall i \neq j$ platí $x_i \neq x_j$.*

Ak začneme tvoriť n-tice od prvého políčka, tak na prvé políčko máme n možností, na druhé $n-1$ možností atď., až nakoniec na posledné políčko nám zostane práve jeden prvok. Takže máme $n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$ rôznych n-tíc. Číslo ktoré dostaneme, označíme $n!$ a voláme n-faktoriál. To znamená, že $n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$ a $0! = 1$. ▪

Poznámka 7 *Ak M je konečná množina a $|M| = n$, a $K = \{1, 2, \cdots, n\}$, tak existuje bijekcia $\psi : K \to M$ (prvky množiny M "očíslujeme"). Množinu M môžeme teraz napísať:*

$$M = \{\psi(1), \psi(2), \cdots, \psi(k)\}.$$

Teda otázka koľko bijekcii existuje na množine K je ekvivalentný s otázkou koľko n-tic vieme vytvoriť z prvkov množiny K tak, že ani jeden sa nebude opakovať. V Poznámke 6 je táto úloha vyriešená. V algebre sa bijekcia na konečnej množine volá tiež permutácia. *Bijekcie vytvárajú grupu s operáciou násobenia (skladania) bijekcii. Nazýva sa tiež* grupa symetrii *resp.* symetrická grupa. *Množina všetkých bijekcií na M sa označuje S_n ($|M| = n$) a $(S_n, \circ)$ sa tiež nazýva symetrická grupa.*

x	f_0	f_1	f_2	f_3	f_4	f_5
a	a	b	c	b	a	c
b	b	c	a	a	c	b
c	c	a	b	c	b	a

Table 4: Bijekcie $f_i : M \to M$, $i = 0, \cdots, 5$.

Príklad 7 *Nech* $M = \{a, b, c\}$. *Vytvorme všetky možné usporiadané trojice:*

$$\{(a,b,c),\ (b,c,a),\ (c,a,b),\ (b,a,c),\ (a,c,b),\ (c,b,a)\}$$

Nech $f_i : M \to M$ *je bijekcia daná tabuľkou 4: Vypočítame* $f_i \circ f_j$ *pre* $\forall i, j$ *pomocou Tab. 4. Napríklad* $f_4 \circ f_2$*:*

$$f_2(f_4(a)) = f_2(a) = c,\ \ f_2(f_4(b)) = f_2(c) = b,\ \ f_2(f_4(c)) = f_2(b) = a,$$

$$f_6 = f_4 \circ f_2 : a \mapsto c,\ \ b \mapsto b,\ \ c \mapsto a.$$

V tabuľke 5 sú všetky $f_i \circ f_j$, $i, j \in \{0, \cdots, 5\}$. *Ak označme* S_3 *množinu*

$\circ$	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_5	f_3	f_4
f_2	f_2	f_0	f_1	f_4	f_5	f_3
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_5	f_3	f_2	f_0	f_1
f_5	f_5	f_3	f_4	f_1	f_2	f_0

Table 5: Všetky možné $f_i \circ f_j$, $i, j \in \{0, \cdots, 5\}$

všetkých bijekcií z M *na* M, *tak* $(S_3, \circ)$ *je grupa, ktorá nie je komutatívna, neutrálny prvok* $I = f_0$ *je identické zobrazenie* $f_0(x) = x$, *pre každé* $x \in M$. *Počet prvkov grupy* $(S_3, \circ)$ *je* $|M|! = 3! = 6$.

Cyklus permutácie – cyklická permutácia

Príklad 8 *Nech* $M = \{0, 1, 2, 3, 4, 5\}$ *a* $f \in S_6$ *(*S_6 *je množina všetkých permutácií na* M*) je v nasledujúcej tabuľke 6:*

M	0	1	2	3	4	5
f	1	3	5	0	4	2

Table 6: Permutácia f na množine M.

Permutáciu f môžeme rozložiť na:

$$\phi_1 = (0, 1, 3), \qquad \phi_2 = (2, 5).$$

Zapíšme do tabuľky všetky tri premutácie f, ϕ_1, a ϕ_2:

M	0	1	2	3	4	5
ϕ_1	1	3	2	0	4	5
ϕ_2	0	1	5	3	4	2
$f = \phi_1 \circ \phi_2$	1	3	5	0	4	2

Table 7: $f = \phi_1 \circ \phi_2 = \phi_2 \circ \phi_1$.

Permutáciam ϕ_1 a ϕ_2 hovoríme cykly.

Definícia 8 *Nech $X = \{x_1, x_2, \cdots, x_k\}$. Bijekciu $\phi : X \to X$ definovanú predpisom*

$$\phi(x_i) = \begin{cases} x_{i+1}, & i < k \\ \\ x_1, & i = k \end{cases}$$

nazývame cyklus a číslo k nazývame dĺžka cyklu. V prípade, že $k = 2$, tak cyklus nazývame transpozícia.

Poznámka 8 *(i) Cyklus ϕ sa zvykne zapisovať pomocou zátvorky:*

$$\phi = (x_1, x_2, \cdots, x_{k-1}, x_k).$$

Z definície vyplýva, že

$$\phi = (x_1, x_2, \cdots, x_k) = (x_2, x_3, \cdots, x_k, x_1) = \cdots (x_k, x_1, \cdots, x_{k-2}, x_{k-1}).$$

(ii) V Príklade 8 sa permutácia f skladá z dvoch cyklov: cyklus ϕ_1 dĺžky 3 a cyklus ϕ_2 dĺžky 2. Alternatívne zápisy:

$$\phi_1 = (0, 1, 3) = (1, 3, 0) = (3, 0, 1), \qquad \phi_2 = (2, 5) = (5, 2).$$

Permutácia ϕ_2 je transpozícia.

Tvrdenie 13 *Každá premutácia sa dá napísať ako súčin transpozícií.*

Dôkaz.
Ak $\phi = (a_1, a_2, \cdots, a_k)$ *je cyklus, potom*

$$\phi = (a_1, a_2, \cdots, a_k) = (a_2, a_3, \cdots, a_k, a_1) \cdots = (a_k, a_1, \cdots, a_{k-1}).$$

Teda postupne presunieme prvok a_1 *na posledné miesto:*

$$\phi = \underbrace{(a_1, a_2)}_{T_1} \circ \underbrace{(a_1, a_3)}_{T_2} \circ \cdots \circ \underbrace{(a_1, a_k)}_{T_{k-1}}.$$

Pretože T_i, $i = 1, \cdots k-1$ *sú transpozície a každá permutácia* f *konečnej množiny* M *s kardinalitou* n *sa dá napísať ako súčin konečného počtu navzájom disjktných cyklov* $\phi_1, \cdots \phi_s$, *kde* $s \leqslant n$, *tak*

$$f = \phi_1 \circ \cdots \circ \phi_s = \underbrace{T_1 \circ \cdots \circ T_{k_1-1}}_{\phi_1} \circ \cdots \circ T_{k_s-1}.$$

∎

Príklad 9 *Zapíšme permutáciu* $f = \phi_1 \circ \phi_2$ *z príkladu 8 pomocou transpozícii: označme*

$$\phi_1 = (0,1,3) \quad \Rightarrow \quad T_1 = (0,1),\ T_2 = (0,3) \quad \Rightarrow \quad \phi_1 = T_1 \circ T_2$$

ϕ_2 *je transpozicia a teda*

M	0	1	2	3	4	5
T_1	1	0	2	3	4	5
T_2	3	1	2	0	4	5
$T_1 \circ T_2$	1	3	2	0	4	5

Table 8: $T_1 \circ T_2 = \phi_1$.

$$f = T_1 \circ T_2 \circ \phi_2.$$

Ale ak zmeníme poradie T_1 *a* T_2 *dostane cyklus* $g = T_2 \circ T_1$

Máme dva cykly $\phi_1 = (0,1,3)$ *a* $\phi_4 = (0,3,1)$.

M	0	1	2	3	4	5
T_2	3	1	2	0	4	5
T_1	1	0	2	3	4	5
$T_2 \circ T_1$	3	0	2	1	4	5

Table 9: $T_1 \circ T_2 \neq T_2 \circ T_1$, tab. 8.

Tvrdenie 14 *Ak cykly ϕ_1, ϕ_2 sú disjuktné, potom $\phi_1 \circ \phi_2 = \phi_2 \circ \phi_1$.*

Dôkaz.

Tvrdenie 15 *Ak cykly ϕ_1, ϕ_2 sú disjuktné, potom $(\phi_1 \circ \phi_2)^n = \phi_1^n \circ \phi_2^n$, pre $n \in Z$.*

Dôkaz.
Keďže binárna operácia $\circ$ je asociatívna a ϕ_1, ϕ_2 sú disjunktné cykly, tak

$$(\phi_1 \circ \phi_2)^n = \underbrace{(\phi_1 \circ \phi_2) \circ (\phi_1 \circ \phi_2) \cdots (\phi_1 \circ \phi_2)}_{n-times} = \phi_1^n \circ \phi_2^n,$$

pre $n \in N$. Ak $n = 0$, tak $I = (\phi_1 \circ \phi_2)^0 = \phi_1^0 \circ \phi_2^0 = I \circ I = I$. Nech $n \leqslant 0$. Označme $k = -n \in N$. Potom

$$(\phi_1 \circ \phi_2)^n = (\phi_1 \circ \phi_2)^{-k} = (\phi_2^{-1} \circ \phi_1^{-1})^k = \phi_1^{-k} \circ \phi_2^{-k} = \phi_1^n \circ \phi_2^n,$$

pretože cykly ϕ_2^{-1}, ϕ_1^{-1} sú disjuktná a teda $\phi_1^{-1} \circ \phi_2^{-1} = \phi_2^{-1} \circ \phi_1^{-1}$. ▪

Definícia 9 *Nech $M = \{a_1, a_2, \cdots, a_n\}$ a permutáciu $f : M \to M$:*

$$f(a_1, a_2, \cdots, a_n) = (f(a_1), \cdots, f(a_n)) = (a_{f_1}, \cdots, a_{f_n}).$$

Nech $i < j$ Inverziou nazveme dvojicu prvkov (a_i, a_j), pre ktorú platí: ak $i < j$, potom $f_i > f_j$.

Permutácia f sa nazýva párna, ak má párny počet inverzií a nepárna, ak má nepárny počet inverzií.

Cvičenie 9 *Nech* $M = \{a_1, a_2, a_3, a_4\}$ *a*

$$f(a_1, a_2, a_3, a_4) = (f(a_1), f(a_2), f(a_3), f(a_4)) = (a_3, a_4, a_1, a_2).$$

$$(1, 2, 3, 4) \to (f_1, f_2, f_3, f_4) = (3, 4, 1, 2).$$

a_3 : $1, 2 < 3$ & $f_3 < f_1, f_2$ *2 inverzie* $(a_3, a_1), (a_3, a_2)$;
a_4 : $1, 2 < 4$ & $f_4 < f_1, f_2$ *2 inverzie* $(a_4, a_1), (a_4, a_2)$;
a_1 : $1 < 2$ & $f_1 < f_2$ *nemá inverzie.*

Permutácia f *je párna, má* 4 *inverzie.*

Poznámka 9 (**Alternatívna podgrupa**) *Ak označíme* P *párnu permutáciu a* N *nepárnu permutáciu, potom pre operáciu* $\circ$ *(skladanie zobrazení) platí:*

$\circ$	P	N
P	P	N
N	N	P

Ak $\mathcal{P}$ *je množina všetkých párnych permutácií a* $\mathcal{N}$ *množina nepárnych permutácii, potom* $(M, \odot)$*, kde* $M = \{\mathcal{P}, \mathcal{N}\}$ *a* $X \odot Y = \{x \circ y;\ x \in X,\ y \in Y\}$*,* $X, Y \in M$*, je grupa izomorfná s grupou* $(Z_2, \oplus_2)$*. Neutrálnym prvkom množina párnych permutácii* $\mathcal{P}$*. Táto grupa sa zvykne nazývať* alternatívna podgrupa.

1.6 Rozklad grupy pomocou podgrupy

Tvrdenie 16 *Nech* $(S, *)$ *je podrupa grupy* $(G, *, e)$*, kde* e *je neutrálny prvok. Ak* $Su = \{x * u, ;\ x \in S\}$*,* $u \in G$*, tak pre* $\forall \in a, b \in G$ *platí, že*

$$Sa = Sb \quad alebo \quad Sa \cap Sb = \varnothing.$$

Naviac $|S| = |Sa|$*, pre* $\forall a \in G$*.*

Dôkaz. *Pretože* $e \in S$*, potom* $e * u \in Su \Rightarrow u \in Su\ \forall u \in G$*.*

Nech $a, b \in G$ *a* $x \in Sa \cap Sb$*. Potom* $\exists s_1, s_2 \in S$

$$s_1 * a = x = s_2 * b \Leftrightarrow$$

$$\Leftrightarrow s_1 = x * a^{-1} \quad \Leftrightarrow \quad s_1 = s_2 * b * a^{-1} \quad \Leftrightarrow \quad s_2^{-1} * s_1 = b * a^{-1}$$

$$b = (s_2^{-1} * s_1) * a \in Sa$$

Nech $x \in S(b)$ *potom* $\exists s_b \in S$

$$x = s_b * b = s_b * ((s_2^{-1} * s_1) * a) = (s_b * s_2^{-1} * s_1) * a \Rightarrow x \in Sa \tag{5}$$

Anologicky z

$$a = (s_2 * s_1^{-1}) * b \in Sb$$

$$y \in Sa \Rightarrow y \in Sb \tag{6}$$

(6) a (5) implikujú $Sa = Sb$. *Teda ak* $Sa \cap Sb \neq \emptyset$, *tak* $Sa = Sb$. ∎

Príklad 10 *Ak* $(G, *) = (Z_{10}, \oplus_{10})$ *a* $S = \{0, 2, 4, 6, 8\}$, *ľahko nahliadneme, že* $(S, \oplus_{10})$ *je podgrupa grupy* G *a platí, že* $S(1) = S(3) = S(5) = S(7) = S(9) = A$, $S(0) = S(2) = S(4) = S(6) = S(8) = S$ *a* $S \cup A = G$. *(Pozri Tab. 10.)*

	$S(0)$	$S(1)$	$S(2)$	$S(3)$	$S(4)$	$S(5)$	$S(6)$	$S(7)$	$S(8)$	$S(9)$
	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
2	2	3	4	5	6	7	8	9	0	1
4	4	5	6	7	8	9	0	1	2	3
6	6	7	8	9	0	1	2	3	4	5
8	8	9	0	1	2	3	4	5	6	7

Table 10: $S(a)$, $a \in G$ (Pr. 10)

Nech $X \oplus Y = \{x \oplus_{10} y;\ x \in X,\ y \in Y\}$, *pre* $X, Y \subset G$ *a* $G_1 = \{A, S\}$. *Potom* $(G_1, \oplus, S) \cong (Z_2, \oplus_2)$. $G_1 = Z_{10}/S$.

$\oplus$	S	A
S	S	A
A	A	S

Cvičenie 10 *Rozložte grupu* $(Z_{15}, \oplus_{15})$ *podľa* $S = \{0, 5, 10\}$.

Riešenie
Ľahko overíme, že $(S, \oplus_{15})$ *je podgrupa* $(Z_{15}, \oplus_{15})$. *Zistíme* $S(x)$, $x \in Z_{15}$. *Dostaneme rozklad množiny* Z_{15} *na* 5 *disjuktných množín* A_i *(analogicky ako v Pr. 10). Ak označíme neutrálny prvok* $S = e$ *a*

$$a_1 = \{1, 6, 11\}, \quad a_2 = \{2, 7, 12\}, \quad a_3 = \{3, 8, 13\}, \quad a_4 = \{4, 9, 14\},$$

potom množina $G = \{e, a_1, a_2, a_3, a_4\}$ *s binárnou operáciou* $\oplus_{15}$ *je izomorfná s grupou* $(Z_5, \oplus_5)$ $((G, \oplus_{15}) \cong (Z_5, \oplus_5))$. ∎

Tvrdenie 17 *Nech* H *je podgrupa grupy* G. $Ha = Hb$ *prave vtedy ak* $ab^{-1} \in H$.

Dôkaz. $\Rightarrow$ *Nech* $Ha = Hb$, *teda pre* $h \in H$ $h \star a \in Hb$ *a teda* $\exists h_a \in H$ $ha = h_a b$. *To implikuje*

$$h_a^{-1} h = b a^{-1}.$$

$$h_a^{-1} h = b a^{-1} \in H$$

$\Leftarrow$ *Ak* $h = ab^{-1} \in H$, *tak* $hb = a \in Hb$ *a* $h^{-1} = ba^{-1} \in H$, *teda*

$$h^{-1} a = b \in Ha$$

$Ha = Hb$. ∎

Tvrdenie 18 *Nech* H *je podgrupa grupy* G. *Ak* $Ha = Hb$, *potom* $Hac = Hbc$ *pre každé* $c \in G$.

Dôkaz.
Podľa Tvrdenia 17 stačí ukázať, že $ac(bc)^{-1} \in H$. *Ale*

$$ac(bc)^{-1} = acc^{-1}b^{-1} = ab^{-1} \in H.$$

∎

Poznámka 10 *Tvrdenie: Ak $Ha = Hb$ potom že pre každé $c \in G$ nemusí vždy platiť: $Hca = Hcb$. Ak by platilo, potom*

$$ca(cb)^{-1} = c(ab^{-1})c^{-1} = chc^{-1} \in H.$$

Poznámka 11 *Kedy bude platiť nasledujúce tvrdenie:*
Ak $x \in Ha$ a $y \in Hb$, potom $xy \in H(ab)$?
Ak $x \in Ha$ a $y \in Hb$, potom existujú prvky $h_x, h_y \in H$ s vlastnosťou, že

$$x = h_x a \quad \& \quad y = h_y b.$$

Hľadáme odpoveď na otázku: Kedy existuje také $h_0 \in H$, že

$$xy = (h_x a)(h_y b) = h_0(ab)?$$

Ak $xy = (h_x a)(h_y b) = h_0(ab)$, tak

$$xy = (h_x a h_y)b = (h_0 a)b \quad \Leftrightarrow \quad h_x a h_y = h_0 a \quad \Leftrightarrow \quad a^{-1} h_x a = h_0 h_y^{-1} \in H.$$

To je pravdaže ekvivalentné s tým, že $aha^{-1} \in H$, pre každé $a \in G$.

Definícia 10 *Podgrupa H grupy G sa nazýva normálna, ak $\forall a \in G \ \forall h \in H$ $aha^{-1} \in H$.*

Poznámka 12 *Ak G je komutatívna grupa (Abelova grupa), potom každá jej podgrupa je normálna.*

1.7 Faktorizácia grupy podľa podgrupy

Nech H je podgrupa grupy G. Potom $\mathcal{H} = \{Ha;\ a \in G\}$ je disjuktny rozklad grupy G. t.z. že $Ha = Hb$, alebo $Ha \cap Hb = \varnothing$. resp. ak $\rho \subset G^2$ a $\rho = \{(x, y) \in G^2;\ \exists h \in H\ y = hx\}$ potom ρ je reláciou ekvivalenie.

Definícia 11 *Nech α je že relácia ekvivalencie. Ak platí:*

$$(a, b), (c, d) \in \alpha \quad \Rightarrow \quad (a * c, b * c) \in \alpha.$$

potom relácia ekvivalencie sa nazýva kongruencia.

Poznámka 13 *a) Ak α je kongruencia a A, B, C sú triedy ekvivalencie, potom pre ľubovoľné $a, b \in A$ a $x, y \in B$*

$$x \star a \in C \quad \Leftrightarrow \quad y \star b \in C.$$

b) Ak H je normálna podgrupa grupy G, potom faktorizácia podľa podgupy H je kongruenciou.

Príklad 11

Nech $M = \{a, b, c, d\}$ a $(G, \circ)$ je grupa všetkých permutácii na M. Nech $f = (a, b, c, d)$ a $g = (a, b)$ sú cykly a $H = \{f^k; k \in Z\}$. Potom $(H, \circ)$ je cyklická podgrupa grupy G. Ak H je normálna podgrupa, potom pre $\forall p \in G$ a $\forall h \in H$ platí:

$$p \circ h \circ p^{-1} \in H,$$

teda aj pre transpozíciu g a premutáciu f. Pretože $g^{-1} = g$, tak

$$g \circ f \circ g^{-1} = g \circ f \circ g$$

a

$$\begin{aligned}(g \circ f \circ g)(a, b, c, d) &= g(f(g(a, b, c, d))) = g(f(b, a, c, d)) \\ &= g(c, b, d, a) = (c, a, d, b) \notin H.\end{aligned}$$

Pripomíname, že množina H má 4 prvky. Tvoria ju len mocniny permutácie f: $H = \{f^0, f, f^2, f^3\}$. To znamená, že H nie je normálna podgrupa grupy G.

1.8 Grupovy homomorfizmus

Definícia 12 *Nech $(G, *, e_G)$, $(H, \circ, e_H)$ sú grupy. Potom zobrazenie*

$$f : G \to H$$

nazývame homomorfizmus (resp. grupovy homomorfizmus), ak pre $\forall a, b \in G$ platí

$$f(a * b) = f(a) \circ f(b).$$

Tvrdenie 19 *: Nech G, H sú grupy a $f : G \to H$ je homomorfizmus. Potom*
a) $f(e_G) = e_H$
b) $\forall a \in G$ $f(a^{-1}) = (f(a))^{-1}$.

Dôkaz.
a) Ak $a \in G$, tak $a = a * e_G$ a teda $f(a) = f(a * e_G)$. Pretože f je grupový homomorfizmus, tak $f(a) = f(a) \circ f(e_G)$. A z rovnice

$$f(a) = f(a) \circ e_H = f(a) \circ f(e_G)$$

vyplýva, že $e_H = f(e_G)$.
b) Ak $a \in G$, tak $a * a^{-1} = e_G$ a teda

$$e_H = f(a * a^{-1}) = f(a) \circ f(a^{-1}) \quad \Rightarrow \quad (f(a))^{-1} = f(a^{-1}).$$

∎

Definícia 13 *Nech $(G, *, e_G)$, $(H, \circ, e_H)$ sú grupy a $f : G \to H$ je homomorfizmus. Potom množina $Ker(f) = \{a \in G;\ f(a) = e_H\}$ sa nazýva jadro homomorfizmu f.*[1]

Tvrdenie 20 *: Nech $(G, *, e_G)$, $(H, \circ, e_H)$ sú grupy a $f : G \to H$ je homomorfizmus. Potom $Ker(f)$ je normálna podgrupa G.*

Dôkaz.
Najskôr ukážeme, že $Ker(f)$ je grupa:

Asociativita: Pretože $Ker(f) \subseteq G$, tak pre dvojicu $(Ker(f), *)$ asociatívny zákon platí.

Uzavretie na binárnu operáciu $*$: Nech $a, b \in Ker(f)$, potom $f(a * b) = h(a) \circ h(b) = e_H \circ e_H = e_H$ a teda $a * b \in Ker(f)$.

Neutrálny prvok: Pretože $e_H = f(e_G)$, tak $e_G \in Ker(f)$.

Existencia inverzného prvku: Nech $a \in Ker(f)$. Potom $e_H = f(e_G) = h(a * a^{-1}) = f(a) \circ f(a^{-1}) = e_H \circ f(a^{-1})$. Teda $f(a^{-1}) = e_H$ a z toho vyplýva, že $a^{-1} \in Ker(f)$.

Takže $Ker(f) \subseteq G$ je podgrupa grupy G. Ešte musíme ukázať, že ide o normálnu podgrupu. To znamená, že $\forall a \in G$ a $\forall u \in Ker(f)$ $a * u * a^{-1} \in Ker(f)$.

Nech $a \in G$ a $u \in Ker(f)$, potom

$$f(a * u * a^{-1}) = f(a) \circ f(u) \circ f(a)^{-1} = f(a) \circ e_H \circ f(a)^{-1} = e_H.$$

Z toho vyplýva, že $a * u * a^{-1} \in Ker(f)$, čo znamená, že $Ker(f)$ je normálna podgrupa. ∎

[1] tu som skoncila 25.3.2019

1.9 Voľné grupy

Nech $X \neq \emptyset$. Množinu X budeme nazývať abeceda. Voľn'a grupa sa nazýva grupa, ktorú vytvorime pomocou abecedy X nasledovne:

1. *Označme nejaký prvok $e \notin X$. Prvok e nazveme neutrálnym prvkom.*
2. *K množine X pridáme jednoprvkovú množinu $\{e\}$: $X \cup \{e\}$.*
3. *Ku každému prvku $a \in X$ pridáme prvok, ktorý označíme a^{-1}. Množinu týchto prvkov označíme X^*.*
4. *Označme $FG(X)$ množinu všetkých slov, ktoré môžeme vytvoriť z množiny $X \cup \{e\} \cup X^*$.*
5. *Zavedieme pravidlo redukcie: $ea = ae = a \ \forall a \in X \cup \{e\} \cup X^*$ a $aa^* = a^*a = e \ \forall a \in X$.*
6. *Zavedieme operáciu reťazenia prvkov $a_i \in X \cup \{e\} \cup X^*$ a $n \in N$: $a_1a_2 \dots a_n$. Reťazec $a_1a_2 \dots a_n = w$ budeme nazývať slovo. Prvok e sa nazýva prázdne slovo. Množina slov $FG(X)$ s pravidlom redukcie a binárnou operáciou reťazenia: $w, u \in FG(X)$, potom $wu, uw \in FG(X)$ tvoria najvšobecnejšiu grupu nad množinou (abecedou) X.*

Príklad 12 *Nech $X = \{2\}$. Potom $FG(X) = \langle\{2\}\rangle = \{2^k;\ k \in Z\}$.*
Čo sme spravili:
Pridali sme k X neutrálny prvok 1 a inverzý k 2, čo je $2^*(= 2^{-1})$. Dostali sme množinu

$$\mathcal{X} = X \cup \{e\} \cup X^* = \{2\} \cup \{1\} \cup \{2^*\}.$$

Potom každý prvok $a \in G$ sa dá napísať ako reťazec nejakých prvkov z $\mathcal{X}$:

$$a = a_1a_2 \cdots a_n \qquad a_i \in \mathcal{X}, \quad i = 1, 2, \dots, n.$$

Napríklad slovo

$$w = 22^*22^*2^*2^* = \underbrace{22^*}_{e}\,\underbrace{22^*}_{e}\,2^*2^* = 2^*2^* = (2^*)^2 = \left(2^{-1}\right)^2 = 2^{-2}$$

To znamená, že $\exists s \in Z$ s vlastnosťou

$$w = a_1a_2 \cdots a_n = 2^s.$$

K prvku (slovu) $a_1a_2 \cdots a_n$ máme redukovaný prvok (redukované slovo) 2^s.

Príklad 13 *Nech $X = \{a, b\}$. Pridajme sme k X neutrálny prvok e a formálne inverzé prvky k a, b, čo je a^{-1}, b^{-1}. Dostali sme množinu*

$$\mathcal{X} = X \cup \{e\} \cup X^* = \{a, b\} \cup \{e\} \cup \{a^{-1}, b^{-1}\}.$$

Potom každý prvok $c \in \langle X \rangle = G$ sa dá napísať ako reťazec prvkov z $\mathcal{X}$:

$$c = c_1 c_2 \cdots c_n \qquad c_i \in \mathcal{X}, \quad i = 1, 2, \ldots, n.$$

Napríklad ak slovo $c = aaabbba^{-1}a^{-1}a^{-1}b^{-1}aa^{-1}b^{-1}bbbbb$ je

$$c = (aaa)(bbb)(a^{-1}a^{-1}a^{-1})(\underbrace{(b^{-1}(aa^{-1})(b^{-1}b)b)}_{e}bbb),$$

potom slovo c v redukovanom tvare je

$$c = a^3b^3a^{-3}b^3$$

konštrukcia voľnej grupy*:*
Nech $X \neq \varnothing$ a $\mathcal{X} = X \cup \{e\} \cup X^*$. Potom každý prvok $c \in FG(X)$ sa dá napísať ako reťazec nejakých prvkov z $\mathcal{X}$:

$$c = a_1^{k_1} \ldots a_n^{k_n},$$

$a_i \in \mathcal{X}$, $i \in Z$, Ak je slovo v redukovanom tvare, potom $a_i \in X \cup X'$. Grupa $FG(X)$ sa nazýva voľná grupa (free group) a od toho označenie $FG(X) = \langle X \rangle$.

Tvrdenie 21 *Nech $X \neq \varnothing$, G je grupa a $f : X \to G$ je zobrazenie. Potom existuje práve jeden homorfizmus z $\phi : FG(X) \to G$ s vlastnosťou, že $\forall x \in X$ $f(x) = \phi(x)$.*

Príklad 14 *Nech $X = \{a, b, c, d\}$ a $G = (Z_6, +)$. Nech*

$$f(a) = f(b) = 1,\ f(c) = 3,\ f(d) = 2.$$

Pretože ϕ je homorfizmus, tak

$$f(a^{-1}) = f(b^{-1}) = 5,\ f(c^{-1}) = 3,\ f(d^{-1}) = 4,$$

a pre $c \in FG(X)$, $c = a_1^{k_1} \ldots a_n^{k_n}$

$$\phi(c) = \phi(a_1^{k_1} \ldots a_n^{k_n}) = \phi(a_1)^{k_1} \ldots \phi(a_n)^{k_n},$$

napr. slovo $a^3b^5acd \in FG(X)$ *pre*

$$\begin{aligned}\phi(a^3b^5acd) =& 3\phi(a) + 5\phi(b) + \phi(a) + \phi(c) + \phi(d) = 3 + 5 + 1 + 3 + 2 = 2.\\ \phi(a^2bc) =& 2\phi(a) + \phi(b) + \phi(c) = 0.\end{aligned}$$

$$\begin{aligned}E = Ker(\phi) =& \{u \in FG(X);\ h(u) = 0\} = \{e, cc, c^{-1}, c^{-1}, ddd, aaaaa, bbbbb \dots\}\\ =& \{e, c^2, c^{-2}, d^3, a^4, b^4, c^2a^4, a^2bc, acd, cad, dac, cbd \dots\}\end{aligned}$$

Popísať všetky prvky nie je možné, ale požívajú sa obecne známe postupy pre konštrukciu grupy. Tvorme teraz triedy:

$$\begin{aligned}F_1 =& \{u \in FG(X);\ h(u) = 1\} = \{a, b, d^2c, a^4c, b^4c, \dots\}\\ F_2 =& \{u \in FG(X);\ h(u) = 2\} = \{a^2, b^2, d, a^4, \dots\}\\ F_3 =& \{u \in FG(X);\ h(u) = 3\} = \{a^3, b^3, c, ad, bd, \dots\}\\ F_4 =& \{u \in FG(X);\ h(u) = 4\} = \{a^4, b^4, \dots\}\\ F_5 =& \{u \in FG(X);\ h(u) = 5\} = \{a^{-1}, b^{-1}, d^{-1}a, \dots\}\end{aligned}$$

Označme $Ew = \{vw;\ v \in E\}$. *Overte že platí:* $w \in F_i$ *práve vtedy, keď* $Ew = F_i$.
Ak $w \in F_i$, *potom pre* $\forall u \in E$

$$h(w) = 0 + i = h(u) + h(w) = h(uw),$$

teda $uw \in Ew$ $(F_i \subseteq Ew)$.*este premysliet*
pre

1.10 Príklady

Príklad 15 *Zistite či* $(M, *)$ *je grupa ak pre nejaké pevne zvolené* $k \in R$

1. $k \neq 0$, $M = R$, $a * b = a + b - kab$;
2. $k \neq 0$, $M = R - \{\frac{1}{k}\}$, $a * b = a + b - kab$;
3. $k \in R$, $M = R$, $a * b = a + b - k$;
4. $M = R - \{0\}$, $a * b = abk$, $k \neq 0$;

5. $k > 0$, $M = \{x + y\sqrt{k};\ x, y \in R\}$, $a * b = a + b$ *(Je to okruh a jednotkou).*

6. $k \neq 0$, $M = R - \{0\}$ $a * b = \frac{a}{b}$

Riešenie:

1. $k \neq 0$, $M = R$, $a * b = a + b - kab$; *Nie je* $(M, *)$ *je grupa. Napríklad ak* $a = \frac{1}{k}$, *potom pre každé* $b \in R$

$$a * b = \frac{1}{k} + b - k\frac{1}{k}b = \frac{1}{k}.$$

Teda rovnica

$$\frac{1}{k} * x = \frac{1}{k}$$

má nekonečne veľa riešení.

2. $k \neq 0$, $M = R - \{\frac{1}{k}\}$, $a * b = a + b - kab$;
Je to grupa: operácia $*$ *je asociatívna,* $e = 0$, $a^{-1} = \frac{a}{ka-1}$.

3. $k \in R$, $M = R$, $a * b = a + b - k$;
Je to grupa: operácia $*$ *je asociatívna,*

$$a * e = a + e - k = a \Rightarrow e = k$$

a

$$k = a^{-1} * a = a^{-1} + a - k \Rightarrow a^{-1} = 2k - a$$

Je to grupa: $e = k$, $a^{-1} = 2k - a$.

4. $M = R - \{0\}$, $a * b = abk$, $k \neq 0$; *Nech* $a, b, c \in R - \{0\}$, *potom Asociatívnosť:*

$$(a * b) * c = k(kab)c = k^2abc$$

$$a * (b * c) = ka(kbc) = k^2abc$$

Neutrálny prvok $a * e = a$

$$a * e = kae = a$$

$$e = \frac{1}{k}.$$

Inverzný prvok $a^{-1} * a = \frac{1}{k}$*:*

$$ka^{-1}a = \frac{1}{k}$$
$$a^{-1} = \frac{1}{k^2 a}.$$

T.z. $(M, *)$ *je grupa.*

5. $k > 0$, $M = \{x + y\sqrt{k};\, x, y \in R\}$, $a * b = a + b$. *Najskôr, ukáěme, že* $*$ *je bin.op.: Nech* $a, b \in M$, *potom*

$$a = x_a + y_a\sqrt{k}, \qquad b = x_b + y_b\sqrt{k}.$$

Teda

$$a * b = (x_a + y_a\sqrt{k}) + (x_b + y_b\sqrt{k}) = (x_a + x_b) + (y_a + y_b)\sqrt{k} \in M.$$

Asociatívnosť:
Neutrálny prvok $a * e = a$

$$a * e = (x_a + y_a\sqrt{k}) + (x_e + y_e\sqrt{k}) = x_a + \sqrt{k}y_a$$
$$x_e + y_e\sqrt{k} = 0,$$

Teda $e = 0 + 0\sqrt{k} = 0$. *Inverzný prvok* $a^{-1} * a = 0$*: ľahko zistíme, že* $a^{-1} = -x_a - y_a\sqrt{k}$. *T.z.* $(M, *)$ *je grupa.*

6. $k \neq 0$, $M = R - \{0\}$ $a * b = \frac{a}{b}$
Asociativita:

$$(a * b) * c = \frac{a}{b} * c = \frac{\frac{a}{b}}{c} = \frac{ac}{b}$$
$$a * (b * c) = a * \frac{b}{c} = \frac{a}{\frac{b}{c}} = \frac{ac}{b}$$

$(M, *)$ *je pologrupa.*
Neutrálny prvok:

$$a * e = a \quad \Rightarrow \quad \frac{a}{e} = a \quad \Rightarrow \quad e = 1$$
$$e * a = a \quad \Rightarrow \quad \frac{e}{a} = a \quad \Rightarrow \quad e = a^2$$

Existuje pravý netrálny, ľavý neexistuje. Nie je to grupa.

Príklad 16 *Nech* $k \neq 0$, $M = R - \{\frac{1}{k}, 0\}$, $a \circ b = \frac{a}{b}$, $a * b = a + b - kab$. *Zistite, či platí distributívny zákon:*

1. $(a * b) \circ c = (a \circ c) * (b \circ c)$
2. $c \circ (a * b) = (c \circ a) * (c \circ b)$
3. $c * (a \circ b) = (c * a) \circ (c * b)$
4. $(a \circ b) * c = (a * c) \circ (b * c)$

Riešenie:

1. $$(a * b) \circ c = \frac{a + b - kab}{c}$$
$$(a \circ c) * (b \circ c) = \frac{a}{c} * \frac{b}{c} = \frac{ac + bc - kab}{c^2}.$$
Teda
$$(a * b) \circ c \neq (a \circ c) * (b \circ c)$$

2. $$c \circ (a * b) = \frac{c}{a * b} = \frac{c}{a + b - kab}$$
$$(c \circ a) * (c \circ b) = \frac{c}{a} * \frac{c}{b} = \frac{ac + bc - kc^2}{ab}$$
$$c \circ (a * b) \neq (c \circ a) * (c \circ b).$$

3. $$c * (a \circ b) = c + \frac{a}{b} - \frac{kac}{b}$$
$$(c * a) \circ (c * b) = \frac{a + c - kac}{b + c - kbc}$$
$c * (a \circ b) \neq (c * a) \circ (c * b)$

4. $$(a \circ b) * c = \frac{a}{b} * c = \frac{a}{b} + c - \frac{kac}{b} = \frac{a + bc - kac}{b}$$
$$(a * c) \circ (b * c) = \frac{a + c - kac}{b + c - kbc}$$
$(a \circ b) * c \neq (a * c) \circ (b * c)$

References

[1] Birkhoff G., Mac Lane S.: Prehľad modernej algebry. Vydavateľstvo technickej a ekonomickej literatúry Alfa, Bratislava, 1977.

[2] Katriňák T., Gavalec M., Gedeonová E., Smital J.: Algebra a teoretická aritmetika. Univerzita Komenského Bratislava, 2002.

[3] Kuroš A., G.: Kapitoly z obecné algebry. Nakladatelství Československé akademie věd, Praha 1968.

[4] Zlatoš P.: Lineárna algebra a geometria. Albert Marenčin PT, spol. s.r.o., Bratislava 2011.