Algebra — cvičení 8, řešení

2. Nechť $(G, \cdot, ^{-1}, 1)$ je grupa a $g \in G$. Dokažte, že pokud prvek $h \in G$ splňuje $h \cdot g = 1$ nebo $g \cdot h = 1$, pak $h = g^{-1}$.

Uvažujme například možnost $g \cdot h = 1$; druhá se ošetří symetrickým argumentem. Vynásobíme-li obě strany rovnosti zleva prvkem g^{-1}, obdržíme $g^{-1} \cdot (g \cdot h) = g^{-1} \cdot 1 = g^{-1}$, kde v druhé rovnosti používáme, že 1 je neutrální prvek. Zbývá jen upravit $g^{-1} \cdot (g \cdot h) = (g^{-1} \cdot g) \cdot h = 1 \cdot h = h$ využívajíce všechny tři grupové axiomy.

3.

Zadání:

	a	b	c	d	e	f
a						
b		c	a	e		
c						
d		f				b
e						
f						

Řešení:

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	e	f	d
c	c	a	b	f	d	e
d	d	f	e	a	c	b
e	e	d	f	b	a	c
f	f	e	d	c	b	a

4. Rozhodněte, zda existuje unární operace $'$ a prvek e takové, aby následující čtveřice byly grupami:

(b) $(\mathbb{Q} \setminus \{0\}, *, ', e)$, kde $a * b = |a \cdot b|$,

(c)* $(\mathcal{P}(X), \Delta, ', e)$, kde $\mathcal{P}(X)$ je množina všech podmnožin množiny X a Δ je symetrická diference: $A \,\Delta\, B = (A \cup B) \setminus (A \cap B)$.

V případě (b) je odpověď záporná. Pro racionální $a < 0$ by totiž muselo v platit $0 > a = a * e = |a \cdot e| \geq 0$, spor.

Odpověď pro (c) je naopak kladná. Pro každé $A \in \mathcal{P}(X)$ definujeme $A' = A$ a položíme $e = \varnothing$. Pak jistě platí $A \,\Delta\, A = e$ a $A \,\Delta\, e = A = e \,\Delta\, A$ pro libovolné $A \in \mathcal{P}(X)$. Komutativita operace Δ je zřejmá, ale nikdo se na ni neptal. Co je netriviální a je potřeba dokázat, je asociativita operace Δ. K tomu je dobré nejprve učinit pozorování, že $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

Pak $(A \,\Delta\, B) \,\Delta\, C = (((A \setminus B) \cup (B \setminus A)) \setminus C) \cup (C \setminus ((A \setminus B) \cup (B \setminus A)))$, což je dále rovno $(A \setminus (B \cup C)) \cup (B \setminus (C \cup A)) \cup (C \setminus (A \cup B)) \cup (A \cap B \cap C)$. To je ovšem výraz symetrický v A, B, C, a tedy je také roven $(B \,\Delta\, C) \,\Delta\, A = A \,\Delta\, (B \,\Delta\, C)$, kde poslední rovnost plyne z komutativity operace Δ.

5. Jaký řád mají následující prvky?

(d) 4 a 15 v $\mathbb{Z}_{75}$,

(e) 7 v $\mathbb{Z}_{20}^*$,

(f) rotace o 144° v $\mathbf{D}_{10}$,

(g) rotace o 144° v $\mathbf{D}_{20}$,

(h) prvek k v kvaternionové grupě $\mathbf{Q}$,

(i) matice $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$, $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$ a $\begin{pmatrix} 0 & 0 & i \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ v $\mathbf{GL}_3(\mathbb{C})$,

(j) dvojice $\big((1\,2\,3)(4\,5), (1\,2\,3\,4)\big)$ v direktním součinu $\mathbf{S}_5 \times \mathbf{S}_4$.

V případě (d) je řád prvku 15 roven 5, jelikož 5 je nejmenší $n \in \mathbb{N}$ takové, že $15n$ je násobek čísla 75, tj. $15n = 0$ v $\mathbb{Z}_{75}$. Stejně tak pro 4 hledáme nejmenší n takové, že $4n$ je násobek čísla 75. Jelikož jsou 4 a 75 nesoudělná přirozená čísla, je nutně $n = 75$.

V případě (e) násobíme 7 samu se sebou, dokud nedostaneme číslo kongruentní s 1 modulo 20. V $\mathbb{Z}_{20}^*$ máme $7 \cdot 7 = 9, 7^3 = 7 \cdot 9 = 3$, $7^4 = 7 \cdot 3 = 1$. Řád prvku 7 je proto roven 4, což většinou zapisujeme $\operatorname{ord}_{\mathbb{Z}_{20}^*} 7 = 4$.

Pro (f) a (g) si stačí uvědomit, že rotaci o 2/5 z 360° je potřeba složit samu se sebou právě pětkrát, abychom dostali násobek 360°, konkrétně 720°. A nezáleží na tom, jestli pracujeme v grupě $\mathbf{D}_{10}$, tj. v grupě symetrií pravidelného pětiúhelníka, či v $\mathbf{D}_{20}$, tj. v grupě symetrií pravidelného 10úhelníka. Podstatné je, že v obou grupách leží inkriminovaná rotace o 144°.

Pro (h) je potřeba si připomenout, že kvaternionová grupa sestává z osmi prvků $1, -1, i, -i, j, -j, k, -k$ a grupovou operací je násobení, které je popsáno následující tabulkou.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Vidíme, že k má řád čtyři, jelikož $k, k^2 = -1, k^3 = -k$ jsou různé od jedné a $k^4 = 1$.

Co se týče matic 3×3, jejich řády postupně jsou $3, 6, \infty, 8$. K tomu asi stačí jen připomenout, že binární operací v grupě $\mathbf{GL}_3(\mathbb{C})$, všech regulárních matic 3×3 nad tělesem $\mathbb{C}$, je násobení. První matice je permutační, která při násobení zleva cyklicky posouvá řádky. Druhá matice je bloková, sestává z jednoho bloku 1×1, kde je prvek -1, a jednoho bloku 2×2, který popisuje otočení v rovině o 120°. Nebýt -1 v bloku 1×1 byl by tedy její řád roven 3, ale takto je roven 6.

Řád třetí matice je ∞, jelikož má determinant (v absolutní hodnotě) větší než 1. Ten se při jejím opakovaném násobení stále zvětšuje a nikdy tedy nemůže být roven 1. Druhá mocnina poslední matice je rovna $\left(\begin{smallmatrix} i & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & i \end{smallmatrix}\right)$. To je prvek řádu čtyři. Původní matice má tedy řád osm.

Zbývá ještě (j), kde řád permutace v první složce je 6, v druhé složce je čtyřcyklus, tj. permutace řádu 4. Řád zadaného prvku je tedy roven $12 = \mathrm{NSN}(6, 4)$.

6. Doplňte následující tabulku, kde v buňce v řádku k a sloupci $\mathbf{G}_n$ bude nejmenší $n \in \mathbb{N}$ takové, že grupa $\mathbf{G}_n$ bude obsahovat prvek řádu k. Předpokládejte, že $\mathbf{D}_{2n}$ je definováno jen pro $n \geq 3$. Řešením je:

	$\mathbf{S}_n$	$\mathbb{Z}_n$	$\mathbf{D}_{2n}$	$\mathbf{GL}_n(\mathbb{R})$	$\mathbf{GL}_n(\mathbb{C})$	$\mathbf{SL}_n(\mathbb{C})$
2	2	2	3	1	1	2
4	4	4	4	2	1	2
11	11	11	11	2	1	2
12	7	12	12	2	1	2
1024	1024	1024	1024	2	1	2

Více si k tomuto příkladu řekneme ve středu na cvičení. Jako šikovné pomocné tvrzení se nám bude hodit, že přiřazení $\psi : a + bi \mapsto \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ definuje prostý okruhový homomorfismus z $\mathbb{C}$ do $\mathbf{M}_2(\mathbb{R})$. Navíc pro každé $z \in \mathbb{C}$ zřejmě platí $\|z\| = \det \psi(z)$.

7. Nechť $(G, \cdot, ^{-1}, 1)$ je *konečná* grupa a H neprázdná podmnožina G. Dokažte, že H tvoří podgrupu G právě tehdy, když je uzavřená na operaci $\cdot$ (tj. $\forall x, y \in H : x \cdot y \in H$).

Jelikož je G konečná, existuje pro každé $g \in G$ nejmenší $n \in \mathbb{N}$ takové, že $g^n = g^m$ pro nějaké $m \in \mathbb{N}$, $m < n$. Zároveň je G grupa, tudíž můžeme obě strany rovnosti přenásobit prvkem $(g^{-1})^m$, abychom obdrželi $g^{n-m} = 1$. Je-li navíc $g \in H$ (připomeňme, že H je neprázdná), plyne (indukcí) z našeho předpokladu, že $1 \in H$. Jistě pak také platí $g^{-1} = g^{n-m-1}$, což je prvek z H, pokud $g \in H$.

8. Nalezněte grupu G a její podmnožinu H, která bude uzavřena na grupovou operaci, ale nepůjde o podgrupu. Například $G = \mathbb{Z}$ (se sčítáním) a $H = \mathbb{N}$.

9. Dokažte, že grupa, ve které má každý nejednotkový prvek řád 2, je už nutně komutativní. Buď $(G, \cdot, ^{-1}, 1)$ taková grupa. Pak pro každé $g, h \in G$ platí $(gh)(gh) = 1$. Po přenásobení prvkem g zleva a prvkem h zprava dostaneme $gghghh = gh$, kde ošklivý výraz nalevo je vzhledem k předpokladu roven $1hg1 = hg$.