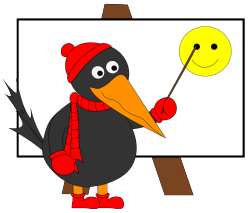
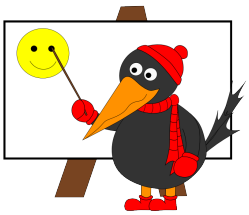


Pomocný text

Grupy



Milí řešitelé,
tentokrát se podíváme na základní stavební kámen vysokoškolské algebry, kterým je teorie grup. Pokud Vám to nic neříká, nezoufejte, vše se Vám pokusíme pěkně pomalu vysvětlit. Nenechte se odradit délkou tohotu textu, velká část jsou jen příklady, které slouží k lepšímu pochopení a získání představy. Základní myšlenkou algebry je pozorování, že různé množiny mají stejnou či podobnou strukturu, přičemž vlastně nezáleží na tom, jaké konkrétní prvky obsahují. Algebra se proto snaží o abstrakci, všímá si podobných vlastností, které dané objekty vykazují. Je nesmírně cenná zejména proto, že formuluje výsledky zcela obecně. I proto má řadu aplikací nejen ve fyzice, v informatice a v chemii. Vlastně i některé věty, které už možná znáte, jsou jen speciálním důsledkem mnohem obecnějších tvrzení.

Počátky teorie grup sahají do posledních let 18. a počátku 19. století; objevují se zde jména jako Euler, Gauss, Lagrange a Galois. První motivací bylo zkoumání vlastností množiny přirozených, celých, racionálních, reálných a komplexních čísel vzhledem k operacím sčítání (popř. odčítání) a násobení (popř. dělení).

Pojďme tedy konečně zjistit, co je to ta grupa. Nejprve ale budeme potřebovat několik definic.

Definice 3.1. *Nechť G je množina. Zobrazení $\clubsuit : G \times G \to G$ se nazývá (binární) operace na množině G.*

Poznámka. Podívejme se podrobněji na pojmy použité v předchozí definici. $G \times G$ značí kartézský součin množiny G se sebou samou. Pokud jsou $g_1, g_2, \ldots, g_n$ prvky G, potom prvky kartézského součinu $G \times G$ jsou *uspořádané* dvojice, např. (g_1, g_1), obecně (g_i, g_j) pro každé i, j, pro která platí $1 \leq i, j \leq n$. Uspořádané znamená, že záleží na pořadí, a proto $(g_i, g_j) \neq (g_j, g_i)$ (rovnost by nastala pouze ve speciálním případě, kdyby platilo $g_i = g_j$).

Operace se nazývá *binární*, protože jejím definiční oborem je kartézský součin $(G \times G)$. Jinými slovy, každým dvěma prvkům z množiny G přiřadí nějaký prvek z G. Pro binární operace se obvykle užívá konvence zápisu $a \clubsuit b$ namísto $\clubsuit((a, b))$.

Příklad 3.1. Operace mohou samozřejmě být i jiné. Jako příklad si definujme *unární* operaci $\square$ (takto ji budeme označovat) na množině přirozených čísel (tu značíme $\mathbb{N} = \{1, 2, \ldots\}$). Tato operace každému přirozenému číslu přiřadí jeho druhou mocninu. Můžeme tedy říci, že zobrazení $\square : \mathbb{N} \to \mathbb{N}$ je definované vztahem $\square(n) = n^2$ pro všechna $n \in \mathbb{N}$. V dalším textu budeme ale uvažovat operace binární.

BRKOS Team 2013

Poznámka. V úvodu jsme zmiňovali operace $+, \cdot$, které by Vám měly být dobře známé. V konkrétních případech tyto operace v teorii grup samozřejmě používáme také, obecně však operace z definice 3.1. nebudeme značit symboly $+, \cdot$, ale např. $\oplus, \otimes, \diamond, *, \clubsuit, \square$. Je dobré označovat operace názorně, jako jsme se o to pokusili v předchozím příkladu. Pro zbytek tohoto textu si zaveďme operaci $\diamond : G \times G \to G$, pod kterou si nemusíte představovat nic konkrétního.

Definice 3.2. *Operace $\diamond$ na množině G se nazývá komutativní, jestliže*

$$a \diamond b = b \diamond a$$

pro libovolné $a, b \in G$, a asociativní, jestliže

$$a \diamond (b \diamond c) = (a \diamond b) \diamond c$$

pro libovolné $a, b, c \in G$.

Poznámka. To, že je operace komutativní, tedy vlastně znamená, že nezáleží na pořadí prvků v této operaci, protože výsledek bude v obou případech stejný. Ne vždy má smysl uvažovat komutativitu, např. u námi zavedené operace $\square$. Příkladem komutativní operace může být opět dobře známá operace $+$ nebo $\cdot$, definovaná na množině celých čísel (tj. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$). Nekomutativní operací může být $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definovaná tak, jak ji znáte. Operace odčítání není komutativní, protože např.

$$8 - 2 = 6 \neq -6 = 2 - 8$$

Asocitivita nám zase říká, že můžeme libovolně přezávorkovat výraz, který obsahuje pouze danou operaci (proto si většinou můžeme dovolit závorky vynechávat). Opět víme, že sčítání a násobení např. na celých číslech je asociativní. Naopak odčítání na celých číslech asociativní není, neboť např.

$$(3 - 2) - 1 = 0 \neq 2 = 3 - (2 - 1).$$

Definice 3.3. *Nechť $\diamond$ je binární operace na množině G. Prvek $e \in G$ se nazývá neutrální či jednotkový prvek (vzhledem k $\diamond$), jestliže*

$$e \diamond a = a \diamond e = a$$

pro libovolné $a \in G$.

Poznámka. Definice takového prvku samozřejmě nezaručuje jeho existenci. Podíváme-li se ovšem opět na operace $+$, $\cdot$, např. na množině $\mathbb{Z}$, tak lehce zjistíme, že takovýto prvek opravdu existuje. Pro $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ (u operace $+$ je zažité označení neutrální prvek) to je 0, protože platí: $\forall z \in \mathbb{Z} : z + 0 = 0 + z = z$. Ve druhém případě $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ (u operace $\cdot$ je častější označení jednotkový prvek) si zkuste ověřit existenci tohoto prvku sami.

Věta 3.1. *Nechť $\diamond$ je binární operace na množině G, potom existuje nejvýše jeden neutrální (jednotkový) prvek vzhledem k $\diamond$.*

Důkaz. Buďte e_1, e_2 jednotkové prvky v G vzhledem k $\diamond$. Pak platí $e_2 = e_1 \diamond e_2$, neboť e_1 je neutrální prvek, a zároveň $e_1 \diamond e_2 = e_1$, neboť i e_2 je neutrální prvek. Tedy $e_1 = e_2$. $\square$

Definice 3.4. *Nechť* $\heartsuit$ *je binární operace na množině* G*,* e *je neutrální prvek vzhledem k* $\heartsuit$ *a* $a \in G$*. Prvek* $b \in G$ *se nazývá inverzní k* a *(vzhledem k* $\heartsuit$*), jestliže*

$$a \heartsuit b = b \heartsuit a = e.$$

Označení 3.1. Inverzním prvkům vzhledem k operaci $+$ říkáme prvky opačné k a. Pro prvek a vzhledem k operaci $+$ značíme opačný prvek $-a$.

U operace $\cdot$ (tj. násobení, jak jej znáte) mluvíme přímo o inverzních prvcích. Pro prvek a značíme opačný prvek a^{-1} (toto označení se obvykle používá pro většinu operací, s výjimkou operace $+$).

Příklad 3.2. K této definici uvedeme pár příkladů. Nechť $+ : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ je operace sčítání na celých číslech, definována tak, jak ji známe. Opačným prvkem ke každému prvku $a \in \mathbb{Z}$ je vzhledem k operaci $+$ prvek $-a$, protože platí

$$a + (-a) = (-a) + a = 0.$$

A o nule víme, že to je neutrální prvek vzhledem k operaci $+$ nad celými čísly.

Buď $\cdot : \mathbb{Q}\times\mathbb{Q} \to \mathbb{Q}$ operace násobení na racionálních číslech $\left(\text{tj. } \mathbb{Q} = \left\{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N}\right\}\right)$ definována předpisem

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

pro každé prvky $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. Snadno nahlédneme, že neutrální prvek operace $\cdot$ je $\frac{1}{1}$, který můžeme psát pouze jako 1. Potom inverzní prvek k prvku $\frac{p}{q}$ je $\frac{q}{p} = \left(\frac{p}{q}\right)^{-1}$, pokud $p \neq 0$. Protože platí

$$\frac{p}{q} \cdot \frac{q}{p} = \frac{pq}{qp} = \frac{\cancel{p}\cancel{q}}{\cancel{q}\cancel{p}} = \frac{\cancel{q}}{\cancel{q}} = \frac{1}{1} = 1$$

pro libovolné $\frac{p}{q} \in \mathbb{Q}, p \neq 0$.

Věta 3.2. *Nechť* $\heartsuit$ *je binární operace na množině* G*, potom ke každému prvku* G *existuje nejvýše jeden* ***inverzní*** *prvek vzhledem k* $\heartsuit$*.*

Důkaz. Buďte b, c prvky inverzní k a. Pak $c = c \heartsuit e = c \heartsuit (a \heartsuit b) = (c \heartsuit a) \heartsuit b = e \heartsuit b = b$. Tedy $b = c$ a k a existuje jen jeden inverzní prvek. □

Nyní se konečně dostáváme k definici grupy.

Definice 3.5. *Uspořádaná dvojice* $(G, \heartsuit)$*, kde* G *je množina a* $\heartsuit$ *je binární operace na* G*, se nazývá grupa, pokud platí následující podmínky:*

- $\heartsuit$ *je na* G *asociativní,*
- *v* G *existuje neutrální prvek vzhledem k* $\heartsuit$*,*
- *ke každému prvku v* G *existuje inverzní prvek vzhledem k* $\heartsuit$*.*

Pokud je navíc $\heartsuit$ *na* G *komutativní, říkáme, že* $(G, \heartsuit)$ *je komutativní grupa. Místo* $(G, \heartsuit)$ *obvykle píšeme stručně pouze* G*, pokud to nevede k nejasnostem. Je-li* G *konečná množina, řádem grupy* G *rozumíme číslo* $|G|$*.*

Poznámka. Pokud bychom v předchozí definici odzdola slevovali z našich podmínek, dostali bychom postupně monoid, pologrupu, resp. grupoid. To jsou všechny algebraické struktury, které lze studovat důkladněji; nás však budou zajímat pouze grupy, protože se chovají „pěkně“ (komutativní ještě pěkněji).

Číslo $|G|$ obecně značí tzv. kardinalitu množiny G. Není to ale nic složitého, u konečné množiny stačí, když si pod $|G|$ představíte počet jejích prvků.

Příklad 3.3. Pojďme se teď společně podívat na různé příklady grup. Pro $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ nebo $\mathbb{C}$ tvoří uspořádaná dvojice $(G, +)$ grupu. Zkusme postupně ověřit platnost podmínek z definice 3.4.

Pro množinu $G = \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ platí, že $\forall a, b \in G : a + b \in G$ a operace je tedy uzavřená na sčítání (tzn. že sečtením dvou prvků z G nemůžeme dostat prvek, který by v G neležel). Ověřme tuto skutečnost pro $G = \mathbb{Q}, \mathbb{C}$. Pro dvě racionální čísla $\frac{a}{b}, \frac{c}{d}$ je sčítání definováno takto

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

a protože $b \neq 0 \neq d$ ani $bd \neq 0$, stejně díky tomu, že $a, c \in \mathbb{Z}$ a $b, d \in \mathbb{N}$ platí $ad + bc \in \mathbb{Z}$. Dohromady jsme tedy dostali, že $\frac{ad+bc}{bd} \in \mathbb{Q}$ a operace je tedy opravdu uzavřená na sčítání.

Nyní proveďme to samé pro komplexní čísla, tj. $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. Sčítání na množině komplexních čísel je definováno na reálné a imaginární složce zvlášť. Spočítejme nyní součet dvou komplexních čísel

$$a + bi + c + di = a + c + bi + di = a + c + (b + d)i$$

a protože $a, b, c, d \in \mathbb{R}$ platí pro výrazy $a + c, b + d \in \mathbb{R}$.

Pro $G = \mathbb{Z}, \mathbb{R}, \mathbb{C}$ snadno nahlédneme, že $+$ je asociativní. Podívejme se, jak to dopadne u $\mathbb{Q}$. Nechť $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$, potom

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + bcf + bde}{bdf}$$

nyní předchozí sčítance uzávorkujme následovně

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{adf + bcf + bde}{bdf}$$

a skutečně, výrazy na pravé straně nám vyšly stejně. Z toho plyne, že $+$ je na $\mathbb{Q}$ asociativní.

S neutrálními prvky je to docela snadné. Pro množinu $\mathbb{Z}$ jsme již takový prvek našli (viz poznámka 3.3.). Pro racionální čísla je to prvek $\frac{0}{1}$, protože $\forall \frac{p}{q} \in \mathbb{Q}$ platí

$$\frac{p}{q} + \frac{0}{1} = \frac{p1 + q0}{q1} = \frac{p}{q}.$$

U reálných čísel je to 0. U koplexních čísel jde o prvek $0 + 0i$, který ale můžeme ztotožnit s 0.

Už nám zbývá jen najít inverzní prvky. Pro $G = \mathbb{Z}, \mathbb{Q}$ jsme tak již učinili v příkladu 3.2. Pro každé $r \in \mathbb{R}$ je jím prvek $-r$, neboť $r + (-r) = 0$. A podobně pro každé $a + bi = z \in \mathbb{Z}$ je jím prvek $-z = -a - bi$, protože platí $z + (-z) = a + bi + (-a - bi) = 0 + 0i$.

Dokonce platí, že uspořádaná dvojice $(G, +)$ tvoří pro $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ komutativní grupu.

Příklad 3.4. Abychom u Vás nevytvořili dojem, že grupu spolu s operací + tvoří kdejaká množina, tak se podívejme na množinu přirozených čísel, tj. $\mathbb{N}$. Můžeme se přesvědčit, že operace + je na $\mathbb{N}$ uzavřená, protože pro každé $a, b \in \mathbb{N}$ totiž platí $a + b \in \mathbb{N}$. Neutrálním prvkem je 0, kterou ovšem v BRKOSu za přirozené číslo nepovažujeme. I kdybychom tak učinili, a měli tak novou množinu $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$, stejně v této množině nebudeme mít inverzní prvky, protože když vybereme libovolný prvek $a \in \mathbb{N}$ (kromě případu $a = 0$, ten inverzi má - sám sebe), máme možnost k němu přičíst pouze nějaké přirozené číslo nebo nulu. Výsledkem libovolného takového součtu ale nikdy nebude 0. Kdybychom se nyní rozhodli přidat k $\mathbb{N}$ i inverzní prvky ke každému prvku $a \in \mathbb{N}$, dostaneme už celá čísla, tj. $\mathbb{Z}$.

Dalším varovným příkladem jsou struktury $(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$, které netvoří grupu, neboť k prvku 0 neexistuje inverzní prvek. Pokud však označíme $G^* = G \setminus \{0\}$ pro $G = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, dostaneme (komutativní) grupu $(G^*, \cdot)$ (detaily si promyslete sami!).

Poznámka. Zkusme se nyní podívat na méně známé množiny. Nechť $n \in \mathbb{N}$ libovolné, označme $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, tedy všechna celá čísla od nuly po $n-1$ včetně. Taková množina se také zavádí jako množina zbytkových tříd po dělení číslem n.

Zbytková třída po dělení číslem n je množina obsahující celá čísla, která dávají stejný zbytek po dělení číslem n. Zvolme například $n = 5$, potom čísla $0, 5, 10$ leží ve stejné zbytkové třídě, protože po dělení pěti dávají zbytek 0 ($0 = 0{\cdot}5{+}0, 5 = 1{\cdot}5{+}0, 10 = 2{\cdot}5{+}0$), podobně čísla $3, 8, -12$ leží ve stejné zbytkové třídě, protože dávají zbytek 3 po dělení pěti ($3 = 0 \cdot 5 + 3, 8 = 1 \cdot 5 + 3, -12 = -3 \cdot 5 + 3$, zbytek musí být kladný). Zbytkovou třídu značíme obvykle nejmenším kladným číslem z dané množiny a pro přehlednost přidáme hranaté závorky.Tedy čísla $0, 5, 10$ leží v třídě $[0]_5$ a čísla $3, 8, -12$ leží v třídě $[3]_5$, přičemž dolní index označuje číslo, kterým jsme dělili, v našem případě 5 (odborně mu říkáme *modul*).

Pro $n = 5$ dostáváme pět zbytkových tříd, a to $[0]_5, [1]_5, [2]_5, [3]_5, [4]_5$. Správně bychom měli psát množinu zbytkových tříd jako $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$, ale pokud to nevede k nejasnostem, je zvykem závorky vynechávat a pracovat s množinou tak, jak jsme ji uvedli na začátku poznámky.

Na množině zbytkových tříd je operace $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ definována následovně: nejdříve počítáme tak, jako kdybychom sčítali celá čísla, ale výsledné číslo podělíme se zbytkem číslem n a podíváme se, do jaké třídy zbytek patří (u takto definované operace bychom měli ověřit její korektnost, tj. jestli $[a_1]_n = [a_2]_n$ a $[b_1]_n = [b_2]_n$, že platí také $[a_1 + b_1]_n = [a_2 + b_2]_n$, to si ovšem dovolíme vynechat). Tuto operaci nazýváme sčítání *modulo* n. Vraťme se k $\mathbb{Z}_5$ a zkusme spočítat $[2]_5 + [7]_5 = [2 + 7]_5 = [4]_5$ nebo $[3]_5 + [3]_5 + [3]_5 + [3]_5 = [3 + 3 + 3 + 3]_5 = [2]_5$ a nakonec $[2]_5 + [-17]_5 = [2 + (-17)]_5 = [-15]_5 = [0]_5$.

Příklad 3.5. Nyní si můžeme uvést další příklad grupy, a to $(\mathbb{Z}_n, +)$, kde $n \in \mathbb{N}$. Z definice této operace je vidět, že je uzavřená na $\mathbb{Z}_n$. Asociativita operace + se přenáší z asociativity operace + na celých číslech. Neutrálním prvkem je třída obsahující nulový prvek, tj. $[0]_n$. Opačným prvkem k prvku $[a]_n$ je prvek $[n - a]_n$, protože $[a]_n + [n - a]_n = [n - a]_n + [a]_n = [0]_n$. Dokonce jde o komutativní grupu (komutativita se opět přenesla z komutativity operace + na celých číslech).

Poznámka. Jedním ze způsobů, jak znázornit grupu, je pomocí tabulky. Nechť $G = \{a, b, c\}$, potom můžeme operaci $\diamond : G \times G \to G$ zavést pomocí tabulky takto:

Je zvykem, že prvně čteme řádek a až poté sloupec. To znamená, že výsledek operace $c \diamond a$ je zapsán v tabulce ve čtvrtém řádku a druhém sloupci a výsledek $a \diamond c$ je zápsán ve

	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

druhém řádku a čtvrtém sloupci. Takto definovaná tabulka nám dává komutativní grupu. Operace $\diamond$ je uzavřena na G, stačí se podívat, že každý prvek v tabulce je z množiny G. Asociativitu bychom museli ověřit pro každou trojici, ale zde ověříme platnost pouze pro trojici a, b, c, tj.

$$(a \diamond b) \diamond c = b \diamond c = a$$
$$a \diamond (b \diamond c) = a \diamond a = a.$$

Neutrálním prvkem je prvek a a inverzní prvky pro a, b, c jsou postupně prvky a, c, b.

Protože jsme všechny předešlé definici vedli v obecné rovině, můžeme pracovat i s dalšími matematickými objekty, tedy ne nutně čísly. Pokusíme se Vám to naznačit v dalším příkladu.

Věta 3.3 (Zákony o krácení.)**.** *Nechť $(G, \diamond)$ je grupa, $a, b, c \in G$. Pak z libovolné z rovností $a \diamond c = b \diamond c$, $\quad c \diamond a = c \diamond b$ vyplývá $a = b$.*

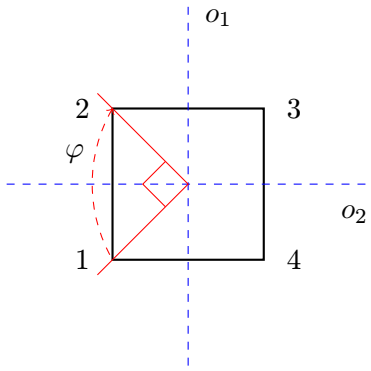
Důkaz. Nechť $a \diamond c = b \diamond c$. Protože $c \in G$ a G je grupa (označme její neutrální prvek e), existuje k c inverzní prvek c^{-1}. Pak

$$a = a \diamond e = a \diamond (c \diamond c^{-1}) = (a \diamond c) \diamond c^{-1} = (b \diamond c) \diamond c^{-1} = b \diamond (c \diamond c^{-1}) = b \diamond e = b.$$

Druhá část se provede zcela analogicky. □

Poznámka. Uvažme nyní pravidelný n-úhelník, kde $n \in \mathbb{N}, n \geq 3$. Ten má pro n liché právě n os symetrií (procházejících vždy jedním vrcholem a středem protější strany) a stejně tak pro n sudé n os symetrií (procházejících vždy dvěma protilehlými vrcholy nebo středy dvojice protilehlých stran). Mimo to ještě můžeme uvažovat n otočení kolem středu o úhel $\frac{2k\pi}{n}$, kde $k = 0, \ldots, n-1$. Symetrie podle osy i otočení kolem středu jsou nějaká rovinná zobrazení. Mějme nyní množinu D všech těchto $2n$ zobrazení pro pravidelný n-úhelník. Označme $\circ$ skládání takovýchto zobrazení. Potom $(D, \circ)$ je grupa, která se nazývá *dihedrální* a zkráceně se značí D_n.

Příklad 3.6. Podrobněji se nyní podívejme na D_4. Z předchozího plyne, že jde o pravidelný čtyřúhelník, tedy čtverec, který má 4 osy symetrie a 4 rotace kolem středu. Dihedrální grupa D_4 má proto 8 prvků. Do následujícího obrázku jsme vyznačili tři z nich, dvě osy symetrie a jednu rotaci (o úhel $\frac{\pi}{2}$).



Skládání zobrazení $\circ$ se vyhodnocuje zprava, tj. v našem případě $\varphi \circ o_2$ znamená nejdříve osovou symterii podle o_2 a až pak rotaci φ. Počítejme nyní, kam se zobrazí postupně prvky $1, 2, 3, 4$ (takto jsme pro větší přehlednost označili jednotlivé rohy, ale pozor, nejsou to prvky D_4!)

$$\begin{aligned}(\varphi \circ o_2)(1) &= \varphi(o_2(1)) = \varphi(2) = 3\\ (\varphi \circ o_2)(2) &= \varphi(o_2(2)) = \varphi(1) = 2\\ (\varphi \circ o_2)(3) &= \varphi(o_2(3)) = \varphi(4) = 1\\ (\varphi \circ o_2)(4) &= \varphi(o_2(4)) = \varphi(3) = 4\end{aligned}$$

Neutrálním prvkem je rotace o 0 stupňů (označme ji id_4), která zřejmě každý prvek nechá na místě. Symetrie jsou samy k sobě inverzní prvky, tedy např. $o_1 \circ o_1 = \mathrm{id}_4 = o_2 \circ o_2$. Pro rotaci o úhel $\frac{2k\pi}{4}$, kde $k = 0, 1, 2, 3$, je inverzním prvkem rotace o úhel $\frac{2(4-k)\pi}{4}$.

Definice 3.6. *Nechť $(G, \circ)$ je grupa s neutrálním prvkem e, a $a \in G$ je libovolný. Potom řád prvku a v grupě $(G, \circ)$ definujeme jako nejmenší přirozené číslo číslo n takové, že $\underbrace{a \circ a \circ \cdots \circ a}_{n} = e$. Pokud takové přirozené číslo neexistuje, řekneme, že řád prvku a je ∞.*

Poznámka. Pro operaci $+$ na $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ dostáváme $\underbrace{a + a + \cdots + a}_{n} = n \cdot a$. Podobně pro operaci $\cdot$ na $G = \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ dostáváme $\underbrace{a \cdot a \cdot \cdots \cdot a}_{n} = a^n$. Proto často výraz $\underbrace{a \circ a \circ \cdots \circ a}_{n}$ nazýváme n-tou mocninou prvku a (pokud se nejedná o operaci $+$, kde by to bylo zavádějící).

Řád prvku a někdy označujeme $\mathrm{ord}(a)$ (z anglického slova *order*) nebo $\mathrm{r}(a)$. Vždy je ale potřeba, aby bylo jasné, v jaké grupě jsme řád prvku počítali.

Hledat řád prvku v nějaké grupě vlastně znamená daný prvek „mocnit“, než dostaneme prvek neutrální. Speciálně neutrální prvek má vždy řád 1 (a je jediný s tímto řádem).

Příklad 3.7. V grupě $(G, +)$, kde $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, má každý prvek kromě neutrálního řád ∞.

Zajímavější je to u grup $(\mathbb{Z}_n, +)$. Zkusme např. spočítat řád prvku $[2]_7$ v $(\mathbb{Z}_7, +)$. Neutrálním prvkem je $[0]_7$, budeme tedy „mocnit“ (v našem případě sčítat) prvek $[2]_7$,

než nám vyjde $[0]_7$.

$$\begin{aligned} [2]_7 + [2]_7 &= [4]_7 \\ [2]_7 + [2]_7 + [2]_7 &= [6]_7 \\ [2]_7 + [2]_7 + [2]_7 + [2]_7 &= [8]_7 \\ &\vdots \\ \underbrace{[2]_7 + [2]_7 + \cdots + [2]_7}_{7} &= [14]_7 = [0]_7 \end{aligned}$$

Dostáváme tak, že řád prvku $[2]_7$ v $(\mathbb{Z}_7, +)$ je 7.

Nyní se vraťme k příkladu 3.6. a podívejme se na řády prvků grupy D_4. Z toho, co jsme si řekli o symetriích, plyne, že každá symetrie má řád 2. Rotace o úhel $\frac{\pi}{2}$ má řád 4, protože když čtyřikrát otočíme čtverec o 90 stupňů podle středu, dostaneme opět ten samý čtverec (jako kdybychom jej otočili o 0 stupňů). Na řády ostatních prvků zkuste přijít sami.

Bez důkazu si uvedeme následující větu:

Věta 3.4 (První důsledek Lagrangeovy věty)**.** *Nechť $(G, \circ)$ je konečná grupa, $a \in G$. Pak řád prvku a dělí řád grupy G.*

Definice 3.7. *Nechť $(G, \circ)$ je grupa, e její neutrální prvek $(G, \circ)$, H podmnožina množiny G. Řekneme, že $(H, \circ)$ je podgrupa grupy G, jestliže jsou splněny následující podmínky:*

- *pokud $a, b \in H$, pak $a \circ b \in H$,*
- *$e \in H$,*
- *pokud $a \in H$, pak v H leží také inverzní prvek k a vzhledem k $\circ$.*

Poznámka. Zkuste si rozmyslet, že každá podgrupa grupy $(G, \circ)$ je sama o sobě grupou (vzhledem ke stejné operaci). Zdědí totiž asociativitu (a případnou komutativitu), všechno ostatní pak vyplývá z definice. Naopak pokud máme grupy $(G, \circ)$ a $(H, \circ)$ takové, že $H \subseteq G$, pak $(H, \circ)$ musí být podgrupou $(G, \circ)$.

Příklad 3.8. Už víme, že $(\mathbb{Z}, +)$ je grupa. Zkusme zjistit, jestli má nějaké podgrupy. Mějme množinu všech sudých celých čísel, označme ji třeba $\mathbb{Z}_S$. Ověřme, jestli platí podmínky z definice 3.7. Platí $\mathbb{Z}_S \subseteq \mathbb{Z}$, navíc víme, že sečtením dvou sudých čísel dostaneme opět sudé číslo. Neutrální prvek je v našem případě 0, ta je sudá, a tedy leží v $\mathbb{Z}_S$. Pokud máme nějaký prvek $a \in \mathbb{Z}_S$, prvek k němu opačný je $-a$, který je určitě zase sudý. Tímto jsme ověřili, že $(\mathbb{Z}_S, +)$ je podgrupa grupy $(\mathbb{Z}, +)$.

Další příklady nám nabízí předchozí poznámka: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ jsou všechno podgrupy grupy $(\mathbb{C}, +)$.

Poslední příklad si rozmyslete sami - v dihedrální grupě $(D_n, \circ)$ tvoří množina všech rotací podgrupu (jako vždy, se stejnou operací).

Na závěr ještě užitečná věta pro konečné grupy, opět bez důkazu:

Věta 3.5 (Druhý důsledek Lagrangeovy věty)**.** *Nechť $(G, \circ)$ je konečná grupa, $(H, \circ)$ její podgrupa. Pak řád H dělí řád G.*

Tak, to je vše. Pokud jste se dočetli až sem, gratulujeme, máte za sebou nejnutnější základy teorie grup! Pokud se Vám tato oblast matematiky zalíbila, vězte, že je velice rozsáhlá a jejím studiem se dá trávit mnoho času. Pokud Vám něco v tomto textu není jasné nebo máte nějaký dotaz, neváhejte se obrátit na `brkos@math.muni.cz`. A teď už vzhůru do řešení třetí série, přejeme Vám hodně štěstí!

BRKOS Team 2013