Algebra I

Radan Kučera, jarní semestr 2012

Literatura, do které míří odkazy z textu:
J. Rosický: **Algebra**, skriptum PřF MU, 4. vydání, Brno 2002 (nebo později), str. 7–102.

Operace na množině, grupoid

Definice. Nechť G je množina. Libovolné zobrazení $G \times G \to G$ se nazývá (binární) **operace** na množině G.

Označení. Operace budeme značit symbolem $\cdot$ (případně $+$, $\circ$, $\bullet$ apod.), obraz dvojice $[a, b] \in G \times G$ v operaci $\cdot$ symbolem $a \cdot b$.

Definice. Operace $\cdot$ na množině G se nazývá

- **komutativní**, jestliže $\forall a, b \in G\colon\ a \cdot b = b \cdot a$;
- **asociativní**, jestliže $\forall a, b, c \in G\colon\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Definice. Množina G spolu s operací $\cdot$ na G se nazývá **grupoid**, označujeme jej $(G, \cdot)$, nebo jen G, bude-li z kontextu jasné, jakou operaci máme na mysli.

Definice. Grupoid $(G, \cdot)$ se nazývá

- **komutativní**, jestliže $\cdot$ je komutativní operace na G;
- **asociativní** (neboli **pologrupa**), jestliže $\cdot$ je asociativní operace na G.

Neutrální prvek, inverzní prvky, grupa

Definice. Nechť $(G, \cdot)$ je grupoid. Prvek $e \in G$ se nazývá **neutrální prvek** (neboli **jednotkový prvek**) tohoto grupoidu, jestliže $\forall a \in G\colon\ e \cdot a = a \cdot e = a$.

Věta. Každý grupoid má nejvýše jeden neutrální prvek. [Věta 1.6, str. 8]

Definice. Nechť $(G, \cdot)$ grupoid s neutrálním prvkem e a nechť je pevně dáno $a \in G$. Prvek $b \in G$ se nazývá **inverzním prvkem** k prvku a (v grupoidu G), jestliže platí $a \cdot b = b \cdot a = e$.

Věta. V libovolné pologrupě s neutrálním prvkem ke každému prvku existuje nejvýše jeden prvek inverzní. [Věta 1.8, str. 8]

Definice. Grupoid G se nazývá **grupa**, jestliže

- G je pologrupa (tj. asociativní grupoid),
- G má neutrální prvek,
- ke každému prvku $a \in G$ existuje v G prvek inverzní.

Označení. V grupě $(G, \cdot)$ tedy ke každému prvku $a \in G$ existuje právě jeden prvek inverzní, značíme jej a^{-1}.

Definice. Je-li $(G, \cdot)$ grupa a je-li navíc operace $\cdot$ komutativní, hovoříme o **komutativní grupě**.

Definice. Grupa $(G, \cdot)$ se nazývá **triviální**, má-li množina G jediný prvek, tj. $G = \{e\}$. (Tento jediný prvek e je pak nutně neutrální, neboť musí platit $e \cdot e = e$.)

Příklad. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy; $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ jsou komutativní grupy, kde $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$, $\mathbb{C}^* = \mathbb{C} - \{0\}$.

Příklad. Nechť R značí kteroukoli z číselných množin $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, pak pro libovolné $m, n \in \mathbb{N}$ definujeme $M_{n,m}(R)$ jako množinu všech matic typu $n \times m$ s prvky z R. Pak $(M_{n,m}(R), +)$ je komutativní grupa (zde $+$ značí sčítání matic).
Naopak $(M_{n,n}(R), \cdot)$, kde $\cdot$ značí násobení matic, je pologrupa s neutrálním prvkem, ale grupa to není. Je-li R kterákoli z číselných množin $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, označme $\mathbb{GL}_n(R)$ množinu všech regulárních matic typu $n \times n$ s prvky z R (tj. matic s nenulovým determinantem). Pak $(\mathbb{GL}_n(R), \cdot)$ je grupa, která není komutativní, je-li $n \geq 2$.

Permutace

Příklad. Nechť X je množina, symbolem X^X značíme množinu všech zobrazení $X \to X$, symbol $\circ$ značí skládání zobrazení. Připomeňme, že pro $f, g \in X^X$ je definováno

$$(f \circ g)(x) = f(g(x)) \qquad \text{pro libovolné } x \in X.$$

Pak $(X^X, \circ)$ je pologrupa s neutrálním prvkem, ale grupa to není.

Definice. **Permutací** na množině X rozumíme libovolnou bijekci $X \to X$. Množinu všech permutací na množině X značíme $\mathbb{S}(X)$. Pokud $X = \{1, 2, \ldots, n\}$, píšeme místo $\mathbb{S}(X)$ stručně jen $\mathbb{S}_n$.

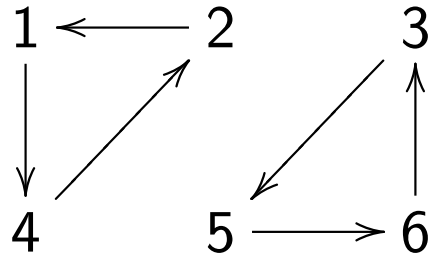
Příklad. $(\mathbb{S}(X), \circ)$ je grupa, která není komutativní, má-li X alespoň tři prvky.

Jak označovat prvky grupy $\mathbb{S}_n$?

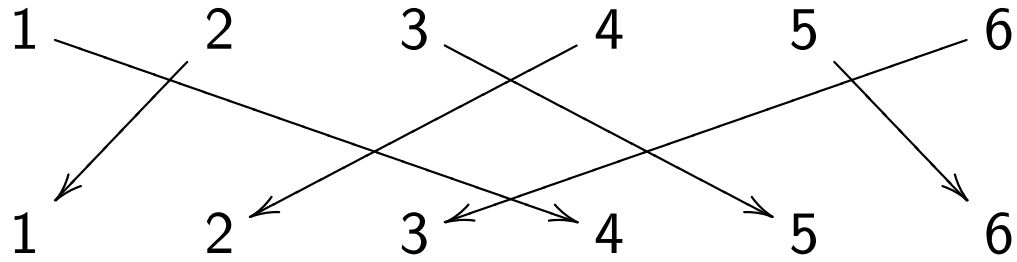
dvouřádkovou maticí

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

orientovaným grafem



anebo schématem



Definice. Nechť $i_1, \ldots, i_k$ jsou různé prvky množiny $\{1, 2, \ldots, n\}$, přičemž $k \geq 2$. Permutaci z $\mathbb{S}_n$ takovou, že

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \quad i_3 \mapsto i_4, \quad \ldots, \quad i_{k-1} \mapsto i_k, \quad i_k \mapsto i_1,$$

přičemž pro všechny prvky $a \in \{1, 2, \ldots, n\}$, $a \notin \{i_1, \ldots, i_k\}$ platí $a \mapsto a$, nazýváme **cyklem délky** k a značíme $(i_1, \ldots, i_k)$. Cykly délky 2 se nazývají **transpozice**.

Definice. Cykly $(i_1, \ldots, i_k), (j_1, \ldots, j_r) \in \mathbb{S}_n$ se nazývají **nezávislé**, jsou-li množiny $\{i_1, \ldots, i_k\}$ a $\{j_1, \ldots, j_r\}$ disjunktní (tj. mají-li prázdný průnik).

Věta. *Každou neidentickou permutaci $f \in \mathbb{S}_n$ lze napsat jako složení několika nezávislých cyklů, a to jednoznačně až na jejich pořadí.* [Věta 2.5, str. 12]

Věta. *Nechť $n > 1$, pak každou permutaci $f \in \mathbb{S}_n$ lze napsat jako složení několika transpozic.* [Věta 2.6, str. 12]

Definice. Nechť $f \in \mathbb{S}_n$. Řekneme, že uspořádaná dvojice $[i, j]$ je **inverze** permutace f, jestliže $1 \leq i < j \leq n$ a platí $f(i) > f(j)$. Permutace f se nazývá **sudá** nebo **lichá** podle toho, má-li sudý nebo lichý počet inverzí. Paritu $p(f)$ permutace f definujeme:

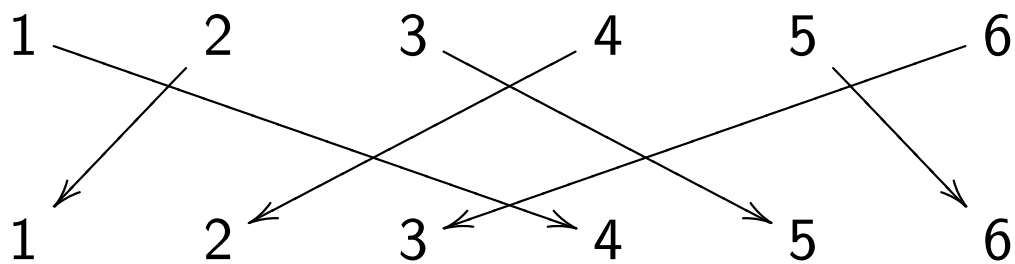
$$p(f) = \begin{cases} 1 & \text{je-li } f \text{ sudá,} \\ -1 & \text{je-li } f \text{ lichá.} \end{cases}$$

Jak zjistit paritu permutace $f \in \mathbb{S}_n$?

Je-li f dána dvouřádkovou maticí, spočítáme, kolikrát ve spodním řádku „je menší číslo předběhnuto větším“:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

$4 > 1$, $4 > 2$, $4 > 3$, $5 > 2$, $5 > 3$, $6 > 3$:
šest inverzí – sudá permutace.
Je-li f dána schématem



spočítáme, kolikrát se protínají šipky:
šest průsečíků - šest inverzí - sudá permutace.

A co parita permutace $f \in \mathbb{S}_n$ zapsané jako složení cyklů?

Věta. *Pro libovolné $f, g \in \mathbb{S}_n$ platí*

$$p(f \circ g) = p(f) \cdot p(g).$$

Jinými slovy: složením libovolných dvou permutací stejné parity dostaneme sudou permutaci, kdežto složením libovolných dvou permutací různé parity dostaneme lichou permutaci. [Věta 2.9, str. 13]

Důsledek. *Složení sudého počtu transpozic je sudá permutace, složení lichého počtu transpozic je lichá permutace.* [Každá transpozice je lichá permutace.]

Důsledek. *Cyklus liché délky je sudá permutace a cyklus sudé délky je lichá permutace.* [Cyklus délky k lze psát jako složení $k - 1$ transpozic.]

Důsledek. *Neidentická permutace je sudá, právě když ve svém rozkladu na složení nezávislých cyklů má sudý počet cyklů sudé délky. Je tedy lichá, právě když v tomto rozkladu má lichý počet cyklů sudé délky. (Na počtu cyklů liché délky nezáleží.)*

Další příklad grupy: grupa $(\mathbb{D}_n, \circ)$

Příklad. Nechť $n \geq 3$ je přirozené číslo a představme si pravidelný n-úhelník. Označme $\mathbb{D}_n$ množinu všech shodností tohoto n-úhelníka, tedy zobrazení, která zachovávají délky úseček a kterými je náš n-úhelník zobrazen sám na sebe. Pak $\mathbb{D}_n$ má $2n$ prvků, z toho n rotací kolem středu n-úhelníka (včetně identity – rotace o nulový úhel) a n osových souměrností (vzhledem k osám procházejících středem n-úhelníka a také dvěma z vrcholů a středů stran). Snadno se ověří, že vzhledem ke skládání dostáváme nekomutativní grupu $(\mathbb{D}_n, \circ)$.
Každá shodnost permutuje množinu vrcholů n-úhelníka, přičemž různým shodnostem odpovídají různé permutace vrcholů. Proto, očíslujeme-li vrcholy n-úhelníka po řadě čísly $1, 2, \ldots, n$, lze každou shodnost n-úhelníka ztotožnit s prvkem grupy $\mathbb{S}_n$. Rotace jsou ztotožněny s mocninami cyklu $(1, 2, \ldots, n)$, každá osová souměrnost je ztotožněna se složením několika nezávislých transpozic.

Dělitelnost v $\mathbb{Z}$

Definice. Říkáme, že celé číslo $b \in \mathbb{Z}$ je dělitelem celého čísla $a \in \mathbb{Z}$, píšeme $b \mid a$, existuje-li $c \in \mathbb{Z}$ tak, že $a = b \cdot c$.

Věta (o dělení se zbytkem). Pro každé $a \in \mathbb{Z}$ a $m \in \mathbb{N}$ existuje jediná dvojice čísel $q, r \in \mathbb{Z}$ takových, že $a = m \cdot q + r$ a současně $0 \leq r < m$. [Věta 3.1, str. 14]

Definice. Číslo q se nazývá **(neúplný) podíl** a číslo r **zbytek** po dělení čísla a číslem m.

Definice. **Společným dělitelem** čísel $a, b \in \mathbb{Z}$ rozumíme každé číslo $c \in \mathbb{Z}$ splňující $c \mid a$ a současně $c \mid b$. Je-li alespoň jedno z čísel a, b nenulové, existuje jen konečně mnoho jejich společných dělitelů; největší z nich se nazývá **největší společný dělitel** čísel a, b, značíme jej (a, b). Jestliže naopak $a = b = 0$, je jejich největší společný dělitel definován jako nula, tj. $(0, 0) = 0$.

Poznámka. Zřejmě platí $(a, b) = (|a|, |b|)$ a $(a, 0) = |a|$, zaměříme se proto na největší společný dělitel přirozených čísel a, b.

Euklidův algoritmus

Pro daná $a, b \in \mathbb{N}$ provádějme postupné dělení se zbytkem:

$$\begin{aligned}
a &= b \cdot q_0 + r_0 \\
b &= r_0 \cdot q_1 + r_1 \\
r_0 &= r_1 \cdot q_2 + r_2 \\
r_1 &= r_2 \cdot q_3 + r_3 \\
&\vdots \\
r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n \\
r_{n-1} &= r_n \cdot q_{n+1} + 0
\end{aligned}$$

Přitom $b > r_0 > r_1 > r_2 > \ldots$, proto skutečně po několika děleních nastane $r_{n+1} = 0$.

Věta. *Pro libovolná $a, b \in \mathbb{N}$ platí* $(a, b) = r_n$. [Věta 3.2, str. 15]

Věta (Bezoutova rovnost). *Pro libovolná $a, b \in \mathbb{Z}$ existují $u, v \in \mathbb{Z}$ tak, že* $(a, b) = u \cdot a + v \cdot b$. [Věta 3.3, str. 16]

Nejmenší společný násobek

Definice. **Společným násobkem** čísel $a, b \in \mathbb{Z}$ rozumíme každé číslo $c \in \mathbb{Z}$ splňující $a \mid c$ a současně $b \mid c$.

Poznámka. Je-li $a = 0$ nebo $b = 0$, je jediným společným násobkem čísel a, b číslo 0. V opačném případě existují kladné společné násobky, například $|a \cdot b|$.

Definice. Jsou-li obě čísla $a, b \in \mathbb{Z}$ nenulová, rozumíme **nejmenším společným násobkem** čísel a, b nejmenšího ze všech kladných společných násobků těchto čísel. Je-li alespoň jedno z čísel a, b nulové, definujeme nejmenší společný násobek čísel a, b jako nulu.

Věta. *Nechť $a, b \in \mathbb{Z}$, $a \neq 0 \neq b$. Pak nejmenším společným násobkem čísel a, b je číslo $\frac{|a \cdot b|}{(a,b)}$. Pro libovolné číslo $c \in \mathbb{Z}$ platí, že c je společným násobkem čísel a, b, právě když c je dělitelné nejmenším společným násobkem čísel a, b.*

Poznámka. Druhá část předchozí věty platí i v případě, kdy je některé z čísel a, b nulové.

Důkaz věty o nejmenším společném násobku

Věta. Nechť $a, b \in \mathbb{Z}$, $a \neq 0 \neq b$. Pak nejmenším společným násobkem čísel a, b je číslo $\frac{|a \cdot b|}{(a,b)}$. Pro libovolné číslo $c \in \mathbb{Z}$ platí, že c je společným násobkem čísel a, b, právě když c je dělitelné nejmenším společným násobkem čísel a, b.

Důkaz. Zřejmě $\frac{|a \cdot b|}{(a,b)} = \pm\frac{b}{(a,b)} \cdot a = \pm\frac{a}{(a,b)} \cdot b$ je společný násobek čísel a, b.

Bezoutova věta dává $u, v \in \mathbb{Z}$ taková, že $(a, b) = u \cdot a + v \cdot b$.

Nechť c je libovolný společný násobek čísel a, b. Pak existují celá čísla x, y tak, že $c = x \cdot a = y \cdot b$. Proto

$$(a, b) \cdot c = u \cdot a \cdot c + v \cdot b \cdot c = a \cdot b \cdot (u \cdot y + v \cdot x),$$

a tedy $c = \frac{a \cdot b}{(a,b)} \cdot (u \cdot y + v \cdot x)$. Tedy c je dělitelné číslem $\frac{|a \cdot b|}{(a,b)}$.

Je-li navíc $c > 0$, plyne odtud, že $c \geq \frac{|a \cdot b|}{(a,b)}$.

Další důsledky Bezoutovy rovnosti

Věta (Bezoutova rovnost). Pro libovolná $a, b \in \mathbb{Z}$ existují $u, v \in \mathbb{Z}$ tak, že $(a, b) = u \cdot a + v \cdot b$.

Následující důsledek vysvětluje, proč jsme dodefinovali $(0, 0) = 0$.

Důsledek. Pro libovolná $a, b, d \in \mathbb{Z}$ platí

$$d \mid (a, b) \quad \Longleftrightarrow \quad d \mid a, \quad d \mid b.$$

Definice. Čísla $a, b \in \mathbb{Z}$ se nazývají **nesoudělná**, jestliže $(a, b) = 1$.

Důsledek. Čísla $a, b \in \mathbb{Z}$ jsou nesoudělná, právě když existují $u, v \in \mathbb{Z}$ tak, že $u \cdot a + v \cdot b = 1$.

Důsledek. Pro libovolná $a, b, c \in \mathbb{Z}$ platí

$$a \mid b \cdot c, \quad (a, b) = 1 \quad \Longrightarrow \quad a \mid c.$$

[Důsledek 3.5, str. 16]

Definice. Přirozené číslo $p > 1$ se nazývá **prvočíslo**, jestliže jeho jediným dělitelem větším než 1 je p samotné.

Důsledek. *Pro libovolné prvočíslo p a libovolná $b, c \in \mathbb{Z}$ platí*

$$p \mid b \cdot c \quad \Longrightarrow \quad p \mid b \quad \text{nebo} \quad p \mid c.$$

Věta (o jednoznačném rozkladu v $\mathbb{Z}$). *Libovolné celé číslo $a > 1$ je buď prvočíslo, nebo jej lze napsat jako součin několika prvočísel, a to jednoznačně až na pořadí činitelů.* [Věta 3.6, str. 16]

Důsledek. *Prvočísel je nekonečně mnoho.* [Jsou-li $p_1, p_2, \ldots, p_n$ všechna prvočísla, neexistuje prvočíslo, které by dělilo číslo $1 + p_1 p_2 \ldots p_n$.]

Důsledek. *Čísla $a, b \in \mathbb{Z}$ jsou nesoudělná, právě když neexistuje prvočíslo p dělící a i b.* [Jsou-li a, b soudělná, nějaké prvočíslo musí dělit číslo $(a, b) > 1$.]

Poznámka. Předchozí větu lze pro malá přirozená čísla užít k hledání největšího společného dělitele tak, že obě čísla rozložíme na součin prvočísel a zjistíme, která prvočísla se vyskytují v obou rozkladech. Obecně však nalézt rozklad na prvočinitele je mnohem obtížnější úkol než nalézt největšího společného dělitele. Celý systém bezpečné komunikace v současnosti je založen na tom, že neumíme rozložit přirozené číslo, které je součinem dvou velkých (řekněme 150-ciferných) prvočísel (výpočet, který by trval několik století, je z praktického hlediska pochopitelně bezcenný).

Kongruence, zbytkové třídy

Definice. Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Říkáme, že a, b jsou **kongruentní** modulo m, a píšeme $a \equiv b \pmod{m}$, jestliže $m \mid a - b$.

Poznámka. Zřejmě $a \equiv b \pmod{m}$, právě když a, b mají stejný zbytek po dělení číslem m.

Definice. Nechť $m \in \mathbb{N}$. Pro libovolné $a \in \mathbb{Z}$ definujeme množinu $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$, kterou nazýváme **zbytková třída** modulo m obsahující a.

Poznámka. Množina $[a]_m = \{a + k \cdot m;\ k \in \mathbb{Z}\}$ se skládá z právě těch celých čísel, která mají stejný zbytek po dělení číslem m jako číslo a.

Věta. *Pro libovolná* $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ *nastává* $[a]_m = [b]_m$ *právě tehdy, když* $a \equiv b \pmod{m}$. [Věta 3.8, str. 17]

Označení. Množinu všech zbytkových tříd podle modulu $m \in \mathbb{N}$ značíme $\mathbb{Z}_m$. Je tedy

$$\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \ldots, [m-1]_m\}.$$

Operace na množině $\mathbb{Z}_m$

Věta. *Nechť $m \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$ jsou libovolná. Jestliže platí $[a]_m = [c]_m$, $[b]_m = [d]_m$, pak také*

$$[a + b]_m = [c + d]_m, \qquad [a \cdot b]_m = [c \cdot d]_m.$$

[Věta 3.9, str. 18]

Důsledek. *Nechť $m \in \mathbb{N}$. Vztahy*

$$[a]_m + [b]_m = [a + b]_m, \qquad [a]_m \cdot [b]_m = [a \cdot b]_m$$

pro libovolná $a, b \in \mathbb{Z}$ definují operace $+$ a $\cdot$ na množině $\mathbb{Z}_m$.

Věta. *Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +)$ komutativní grupa s neutrálním prvkem $[0]_m$, v níž inverzním prvkem k libovolné třídě $[a]_m$ je třída $[-a]_m$.* [Věta 3.11, str. 19]

Věta. *Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, \cdot)$ komutativní pologrupa s neutrálním prvkem $[1]_m$.* [Věta 3.12, str. 19]

Poznámka. Jestliže $m > 1$, pro každé $a \in \mathbb{Z}$ platí $[a]_m \cdot [0]_m = [a \cdot 0]_m = [0]_m \neq [1]_m$, a tedy $(\mathbb{Z}_m, \cdot)$ není grupa.

Grupa $(\mathbb{Z}_m^\times, \cdot)$

Věta. *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná. Zbytková třída $[a]_m$ má inverzní prvek v pologrupě $(\mathbb{Z}_m, \cdot)$, právě když celá čísla a, m jsou nesoudělná.* [Věta 3.13, str. 19]

Označení. Pro libovolné $m \in \mathbb{N}$ označme $\mathbb{Z}_m^\times$ množinu všech zbytkových tříd $[a]_m$, které mají inverzní prvek v pologrupě $(\mathbb{Z}_m, \cdot)$, tedy

$$\mathbb{Z}_m^\times = \{[a]_m;\ a \in \mathbb{Z},\ (a, m) = 1\}.$$

Důsledek. *Pro každé $m \in \mathbb{N}$ je $(\mathbb{Z}_m^\times, \cdot)$ komutativní grupa.*

Označení. Pro libovolné $m \in \mathbb{N}$ označme $\varphi(m)$ počet všech přirozených čísel nepřevyšujících m, která jsou nesoudělná s m, tedy

$$\varphi(m) = |\{a \in \mathbb{Z};\ 0 < a \leq m,\ (a, m) = 1\}|.$$

Důsledek. *Pro libovolné $m \in \mathbb{N}$ platí $|\mathbb{Z}_m^\times| = \varphi(m)$.*

Definice. Výše definované zobrazení $\varphi : \mathbb{N} \to \mathbb{N}$ se nazývá **Eulerova funkce**.

První věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Je-li p prvočíslo a $n \in \mathbb{N}$, pak* $\varphi(p^n) = (p-1) \cdot p^{n-1}$.

Důkaz. Čísla soudělná s p^n jsou právě ta, která jsou dělitelná p.

Z každých p po sobě jdoucích čísel je právě jedno dělitelné p.

Proto je mezi čísly $1, 2, \ldots, p^n$ právě $\frac{p^n}{p} = p^{n-1}$ čísel, která jsou soudělná s p^n.

Nesoudělných s p^n je mezi nimi právě $\varphi(p^n)$ čísel.

Je tedy $\varphi(p^n) = p^n - p^{n-1} = (p-1) \cdot p^{n-1}$.

Druhá věta o Eulerově funkci $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Jsou-li $a, b \in \mathbb{Z}$ nesoudělná celá čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Důkaz. Protože $(a, b) = 1$, nejmenší společný násobek čísel a, b je $a \cdot b$. Definujme zobrazení $f : \mathbb{Z}_{ab} \to \mathbb{Z}_a \times \mathbb{Z}_b$ předpisem $f([c]_{ab}) = ([c]_a, [c]_b)$ pro libovolné $c \in \mathbb{Z}$.
Je třeba ověřit korektnost této definice: pro libovolné $c, d \in \mathbb{Z}$ platí $[c]_{ab} = [d]_{ab}$, právě když $ab \mid c - d$.
Protože ab je nejmenší společný násobek čísel a, b, platí $ab \mid c - d \;\Leftrightarrow\; a \mid c - d \;\wedge\; b \mid c - d$.
Celkem tedy $[c]_{ab} = [d]_{ab} \;\Leftrightarrow\; ([c]_a, [c]_b) = ([d]_a, [d]_b)$.
Ověřili jsme nejen korektnost definice f, ale i to, že f je injektivní.
A protože množiny $\mathbb{Z}_{ab}$ i $\mathbb{Z}_a \times \mathbb{Z}_b$ mají obě ab prvků, je f bijekce.
Libovolné $c \in \mathbb{Z}$ splňuje $(c, ab) \neq 1$, právě když existuje prvočíslo p tak, že $p \mid c$ a současně $p \mid ab$, tj. že $p \mid c$, $p \mid a$ nebo $p \mid c$, $p \mid b$, tj. právě když $(c, a) \neq 1$ nebo $(c, b) \neq 1$. Celkem tedy $[c]_{ab} \in \mathbb{Z}_{ab}^\times$, právě když $f([c]_{ab}) \in \mathbb{Z}_a^\times \times \mathbb{Z}_b^\times$. Proto $|\mathbb{Z}_{ab}^\times| = |\mathbb{Z}_a^\times| \cdot |\mathbb{Z}_b^\times|$.

Výpočet hodnot Eulerovy funkce $\varphi(m) = |\mathbb{Z}_m^\times|$

Příklad. Předpoklad o nesoudělnosti je v předchozí větě podstatný, platí třeba $\varphi(2 \cdot 2) = 2 \neq 1 = \varphi(2) \cdot \varphi(2)$.

Důsledek. *Nechť $m \in \mathbb{N}$. Rozložme m na součin mocnin různých prvočísel, tj.*

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s},$$

kde $p_1, p_2, \ldots, p_s$ jsou různá prvočísla, $e_1, e_2, \ldots, e_s \in \mathbb{N}$. Pak platí

$$\varphi(m) = (p_1 - 1) \cdot p_1^{e_1 - 1} \cdot (p_2 - 1) \cdot p_2^{e_2 - 1} \cdots (p_s - 1) \cdot p_s^{e_s - 1},$$

což je možné zapsat také takto:

$$\varphi(m) = m \cdot \prod_{\text{prvočíslo } p \mid m} \left(1 - \tfrac{1}{p}\right).$$

Základní vlastnosti grup, mocnina v pologrupě

Věta. *Nechť $(G, \cdot)$ je pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ (v tomto pořadí) nezáleží na jejich uzávorkování.* [Věta 4.1, str. 23]

Věta. *Nechť $(G, \cdot)$ je komutativní pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ nezáleží na jejich pořadí.* [Věta 4.2, str. 24]

Definice. Nechť $(G, \cdot)$ je pologrupa, $a \in G$, $n \in \mathbb{N}$. **Mocninu** a^n prvku a v pologrupě G definujeme jako součin n exemplářů prvku a:

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n}$$

(podle výše uvedené věty není nutné specifikovat uzávorkování).

Věta. *Nechť $(G, \cdot)$ je pologrupa, $a \in G$, $m, n \in \mathbb{N}$. Pak platí* $a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{m \cdot n}$. [Věta 4.4, str. 24]

Invertibilní prvky

Označení. Nechť $(G, \cdot)$ je grupoid s neutrálním prvkem. Víme, že tento neutrální prvek je v G jediný. Budeme jej označovat symbolem 1 (přestože to nemusí být přirozené číslo 1).

Definice. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1. Pokud k nějakému $a \in G$ existuje v G prvek inverzní, říkáme, že prvek a je **invertibilní**. Inverzní prvek k prvku a budeme označovat symbolem a^{-1}.

Věta. *Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1, $a, a_1, \ldots, a_n$ libovolné invertibilní prvky z G. Pak platí*

$$\begin{aligned} 1^{-1} &= 1, \\ (a^{-1})^{-1} &= a, \\ (a_1 \cdot \ldots \cdot a_n)^{-1} &= a_n^{-1} \cdot \ldots \cdot a_1^{-1}. \end{aligned}$$

[Věta 4.6, str. 24]

Věta (zákony o krácení). *Nechť G je grupa, $a, b, c \in G$. Pak platí*

$$\begin{aligned} a \cdot b = a \cdot c \quad &\Longrightarrow \quad b = c, \\ b \cdot a = c \cdot a \quad &\Longrightarrow \quad b = c. \end{aligned}$$

[Věta 4.17, str. 27]

Množina všech invertibilních prvků pologrupy, mocnina v grupě

Věta. *Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1, H množina všech invertibilních prvků z G. Pak $(H, \cdot)$ je grupa.* [Věta 4.7, str. 25]

Poznámka. Operace $\cdot$ na množině H je zúžením původní operace na množině G (má stejný předpis, ale je definována na menším definičním oboru $H \times H$ a má menší obor hodnot H).

Poznámka. Předchozí větu jsme už několikrát použili: na pologrupách čtvercových matic $(M_{n,n}(R), \cdot)$, zobrazení $(X^X, \circ)$ a zbytkových tříd $(\mathbb{Z}_m, \cdot)$. Vznikly grupy $\mathbb{GL}_n(R)$, $\mathbb{S}(X)$ a $\mathbb{Z}_m^\times$.

Definice. Nechť $(G, \cdot)$ je grupa s neutrálním prvkem 1, $a \in G$. **Mocninu** a^n prvku a v grupě G definujeme i pro nekladný celočíselný exponent: $a^0 = 1, \quad a^{-n} = (a^n)^{-1}$ pro libovolné $n \in \mathbb{N}$.

Věta. *Nechť $(G, \cdot)$ je grupa, $a \in G$, $m, n \in \mathbb{Z}$. Pak platí* $a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{m \cdot n}$. [Věta 4.9, str. 25]

Věta. *Nechť $(G, \cdot)$ je komutativní grupa, $a, b \in G$, $m \in \mathbb{Z}$. Pak platí* $(a \cdot b)^m = a^m \cdot b^m$. [Věta 4.10, str. 26]

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G. Neexistuje-li žádné přirozené číslo n s touto vlastností, říkáme, že řád prvku a v grupě G je ∞.

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \iff k \equiv l \pmod{n}.$$ [Věta 4.13 (1) a (2), str. 26]

Je-li naopak řád prvku a v grupě G roven ∞, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \iff k = l.$$ [Věta 4.13 (3), str. 26]

Důsledek. *Nechť řád prvku a v grupě G je $n \in \mathbb{N}$. Nechť r je zbytek po dělení čísla $k \in \mathbb{Z}$ číslem n, pak $a^k = a^r$. Prvky $a^0 = 1$, $a^1 = a$, a^2, $\ldots$, a^{n-1} jsou po dvou různé.*

Důsledek. *Řád prvku a v grupě G tedy udává, kolik existuje různých mocnin prvku a. V konečné grupě má každý prvek konečný řád.*

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.*

Věta. *Nechť G je komutativní grupa, $a, b \in G$ takové, že řád prvku a je $m \in \mathbb{N}$, řád prvku b je $n \in \mathbb{N}$. Jestliže $(m, n) = 1$, pak řád prvku $a \cdot b$ je $m \cdot n$.*

Důkaz. Jistě $(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = 1^n \cdot 1^m = 1$. Nechť pro $t \in \mathbb{N}$ platí $(a \cdot b)^t = 1$. Pak $1 = (a \cdot b)^{tm} = (a^m)^t \cdot b^{tm} = b^{tm}$, a tedy $n \mid tm$, což vzhledem k $(m, n) = 1$ dává $n \mid t$. Analogicky $m \mid t$. Celkem z $(m, n) = 1$ dostaneme $mn \mid t$.

Exponent konečné grupy

Definice. Nechť G je konečná grupa. Nejmenší $e \in \mathbb{N}$ takové, že pro každé $a \in G$ platí $a^e = 1$, se nazývá **exponent** grupy G.

Poznámka. Máme-li konečnou grupu G, můžeme určit řád každého prvku grupy G a spočítat nejmenší společný násobek všech získaných řádů. Tento nejmenší společný násobek je roven exponentu grupy G.

Věta. Nechť G je konečná komutativní grupa. Pak exponent grupy G je roven největšímu z řádů všech prvků grupy G.

Důkaz. Označme S množinu řádů prvků grupy G a $m = \max S$. Předpokládejme, že existuje $k \in S$, $k \nmid m$. Z jednoznačnosti rozkladu na prvočísla víme, že existuje prvočíslo p tak, že $p^r \mid k$, $p^r \nmid m$, pro nějaké $r \in \mathbb{N}$. Rozepišme $m = p^c \cdot n$, $p \nmid n$, pak $c < r$. Platí $p^r \in S$, $n \in S$, $(p^r, n) = 1$ a G je komutativní. Proto $p^r \cdot n \in S$ a $p^r \cdot n > m$, spor.

Příklad. Exponent grupy $\mathbb{S}_3$ je 6, přitom v $\mathbb{S}_3$ prvek řádu 6 není. Předpoklad, že G je komutativní, je v předchozí větě nutný.

Podgrupa grupy

Definice. Nechť $(G, \cdot)$ je grupa, H podmnožina množiny G. Řekneme, že H je podgrupa grupy G, a píšeme $H \leq G$, jestliže

- neutrální prvek $1 \in H$,
- pro každé $a \in H$ platí $a^{-1} \in H$,
- pro každé $a, b \in H$ platí $a \cdot b \in H$.

Poznámka. Největší podgrupou grupy G (vzhledem k $\subseteq$) je celá G, nejmenší podgrupou je $\{1\}$.

Věta. *Nechť H je podgrupa grupy $(G, \cdot)$. Pak $\cdot$ určuje operaci na množině H, přičemž H je grupa vzhledem k této operaci. Je-li grupa G komutativní, pak je i grupa H komutativní.* [Věta 5.3, str. 29]

Označení. Zmiňovanou operaci na podgrupě budeme označovat stejným symbolem jako původní operaci na celé grupě, přestože tyto operace nejsou stejné.

Věta. *Jestliže H je podgrupa grupy G a K je podgrupa grupy H, pak je K také podgrupou grupy G.* [To je zřejmé.]

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť G je grupa, I neprázdná množina taková, že pro každé $i \in I$ je dána podgrupa H_i grupy G. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podgrup je opět podgrupou grupy G.* [Věta 5.5, str. 29]

Definice. Nechť M je podmnožina grupy G. Symbolem $\langle M \rangle$ označíme průnik všech podgrup grupy G, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podgrupou grupy G obsahující množinu M; evidentně je nejmenší s touto vlastností. Podgrupu $\langle M \rangle$ nazýváme **podgrupa generovaná množinou** M, množinu M nazýváme **množina generátorů podgrupy** $\langle M \rangle$.

Označení. Je-li $M = \{a_1, \ldots, a_n\}$, lze psát stručně $\langle a_1, \ldots, a_n \rangle$ místo $\langle M \rangle$.

Poznámka. Zřejmě $\langle G \rangle = G$, $\langle \emptyset \rangle = \{1\}$. Pro každou $M \subseteq G$ platí

$$\langle M \rangle = \langle M \cup \{a^{-1};\ a \in M\} \rangle.$$

Podgrupa grupy generovaná podmnožinou grupy

Věta. *Nechť M je podmnožina grupy $(G, \cdot)$ taková, že $M \neq \emptyset$ a že pro každé $a \in M$ je také $a^{-1} \in M$. Pak platí*

$$\langle M \rangle = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}.$$

Důkaz. Označme $X = \{a_1 \cdot \ldots \cdot a_n;\ n \in \mathbb{N},\ a_1, \ldots, a_n \in M\}$.

Jistě $M \subseteq X$ (volbou $n = 1$).

Protože $M \neq \emptyset$, existuje $b \in M$, pak i $b^{-1} \in M$ a $1 = b \cdot b^{-1} \in X$.
Pro libovolné $c = a_1 \cdot \ldots \cdot a_n \in X$ je $c^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1} \in X$.
Protože součin n prvků z M vynásobený součinem m prvků z M je součinem $n + m$ prvků z M, je X uzavřeno na operaci $\cdot$.
Je tedy X podgrupa grupy G.

Naopak libovolná podgrupa Y grupy G obsahující M obsahuje také libovolný součin prvků z M, proto $X \subseteq Y$.

Je tedy X nejmenší podgrupa grupy G obsahující M, tj. $X = \langle M \rangle$.

Cyklické grupy

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$. Pak platí* $\langle a \rangle = \{a^m;\ m \in \mathbb{Z}\}$. [Stačí užít větu pro $M = \{a, a^{-1}\}$ spolu s $\langle a \rangle = \langle a, a^{-1} \rangle$.]

Důsledek. *Nechť $(G, \cdot)$ je grupa, $a \in G$ je prvek řádu $n \in \mathbb{N} \cup \{\infty\}$. Pak počet prvků podgrupy $\langle a \rangle$ generované prvkem a je roven n.*

[Víme, že řád prvku a v grupě G udává, kolik existuje různých mocnin prvku a.]

Definice. Grupa G se nazývá **cyklická**, existuje-li $a \in G$ tak, že $G = \langle a \rangle$.

Příklad. Grupy $(\mathbb{Z}, +)$ i $(\mathbb{Z}_m, +)$ pro libovolné $m \in \mathbb{N}$ jsou cyklické.

Definice. Řádem konečné grupy $(G, \cdot)$ rozumíme počet prvků této grupy, značíme $|G|$.

Důsledek. *Řád konečné cyklické grupy je roven řádu jejího generátoru. Konečná grupa řádu n je cyklická, právě když obsahuje prvek řádu n.*

[Obsahuje-li konečná grupa řádu n prvek a řadu n, má podgrupa $\langle a \rangle$ stejný počet prvků jako G, tedy $\langle a \rangle = G$.]

Důsledek. *Nechť H, K jsou podgrupy komutativní grupy $(G, \cdot)$. Pak platí* $\langle H \cup K \rangle = \{h \cdot k;\ h \in H,\ k \in K\}$. [Důsledek 5.9, str. 30]

Homomorfismus grup

Definice. Nechť $(G_1, \cdot)$ a $(G_2, *)$ jsou grupy, $f : G_1 \to G_2$ zobrazení. Řekneme, že f je **homomorfismus** grupy $(G_1, \cdot)$ do grupy $(G_2, *)$, jestliže pro každé $a, b \in G_1$ platí $f(a \cdot b) = f(a) * f(b)$. Injektivní homomorfismus se nazývá **vnoření**, bijektivnímu homomorfismu říkáme **izomorfismus**.

Poznámka. Nepřesně řečeno: homomorfismus je zobrazení mezi grupami, u kterého dostaneme totéž, ať už „*napřed počítáme a pak zobrazujeme*“ anebo „*napřed zobrazujeme a pak počítáme*“.

Příklad. Pro libovolné $m \in \mathbb{N}$ je zobrazení parita $p : \mathbb{S}_m \to \{1, -1\}$ homomorfismus grupy permutací $(\mathbb{S}_m, \circ)$ do grupy $(\{1, -1\}, \cdot)$, neboť pro libovolné permutace $f, g \in \mathbb{S}_m$ platí $p(f \circ g) = p(f) \cdot p(g)$. V případě $m = 2$ jde o izomorfismus.

Příklad. Zobrazení logaritmus $\log : \mathbb{R}^+ \to \mathbb{R}$ je homomorfismus multiplikativní grupy všech kladných reálných čísel $(\mathbb{R}^+, \cdot)$ do aditivní grupy všech reálných čísel $(\mathbb{R}, +)$, neboť pro libovolná kladná reálná čísla a, b platí $\log(a \cdot b) = (\log a) + (\log b)$. Protože je toto zobrazení bijekce, jde o izomorfismus.

Homomorfismus grup

Definice. Nechť $(G_1, \cdot)$ a $(G_2, *)$ jsou grupy. Zobrazení $f : G_1 \to G_2$ se nazývá **homomorfismus**, jestliže pro každé $a, b \in G_1$ platí $f(a \cdot b) = f(a) * f(b)$. **Vnoření** je injektivní homomorfismus, **izomorfismus** je bijektivní homomorfismus.

Příklad. Pro libovolné $m \in \mathbb{N}$ je determinant $\det : \mathbb{GL}_m(\mathbb{R}) \to \mathbb{R}^*$ homomorfismus grupy regulárních matic typu $m \times m$ s reálnými prvky $(\mathbb{GL}_m(\mathbb{R}), \cdot)$ do grupy nenulových reálných čísel $(\mathbb{R}^*, \cdot)$. Pro libovolné matice $A, B \in \mathbb{GL}_m(\mathbb{R})$ totiž podle Cauchyovy věty platí $\det(A \cdot B) = \det(A) \cdot \det(B)$. V případě $m = 1$ jde o izomorfismus.

Věta. Jsou-li G_1, G_2, G_3 grupy, $f : G_1 \to G_2$ a $g : G_2 \to G_3$ homomorfismy, pak je $g \circ f : G_1 \to G_3$ homomorfismus. [Věta 8.3, str. 41]

Věta. Nechť $f : G_1 \to G_2$ je homomorfismus grup. Pak $f(1) = 1$ a pro každé $a \in G_1$ platí $f(a^{-1}) = f(a)^{-1}$. [Věta 8.4, str. 41]

Věta. Nechť $f : G_1 \to G_2$ je izomorfismus grup. Pak i inverzní zobrazení $f^{-1} : G_2 \to G_1$ je izomorfismus grup. [Věta 6.3, str. 33]

Homomorfismus grup, jeho jádro

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, $a \in G_1$ prvek řádu $n \in \mathbb{N}$. Pak řád prvku $f(a)$ v grupě G_2 je $k \in \mathbb{N}$ a platí $k \mid n$.*

[Jestliže $a^n = 1$, pak $(f(a))^n = f(a^n) = f(1) = 1$, a proto řád k prvku $f(a)$ je dělitelem čísla n.]

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup. Pak obraz $f(G_1) = \{f(a);\ a \in G_1\}$ grupy G_1 je podgrupou grupy G_2.* [Věta 8.5, str. 42]

Věta. *Nechť $f : G_1 \to G_2$ je homomorfismus grup, H podgrupa grupy G_2. Pak úplný vzor $f^{-1}(H) = \{a \in G_1;\ f(a) \in H\}$ podgrupy H je podgrupou grupy G_1.* [Věta 8.9, str. 42]

Definice. Nechť $f : G_1 \to G_2$ je homomorfismus grup. Množina $\ker f = \{a \in G_1;\ f(a) = 1\}$ se nazývá **jádro homomorfismu** f.

Důsledek. *Je-li $f : G_1 \to G_2$ je homomorfismus grup, pak jeho jádro $\ker f$ je podgrupa grupy G_1.*

Věta. *Homomorfismus grup $f : G_1 \to G_2$ je injektivní, právě když $\ker f = \{1\}$.* [Věta 8.11, str. 43]

Příklad. *Popište všechny homomorfismy $\mathbb{S}_3 \to \mathbb{Z}_4$ a jejich jádra.*

V grupě $\mathbb{S}_3$ má neutrální prvek id řád 1, transpozice $(1,2)$, $(1,3)$ a $(2,3)$ řád 2 a cykly $(1,2,3)$ a $(1,3,2)$ řád 3. V grupě $\mathbb{Z}_4$ má neutrální prvek $[0]_4$ řád 1, prvek $[2]_4$ řád 2, prvky $[1]_4$ a $[3]_4$ řád 4. Protože v $\mathbb{Z}_4$ není prvek řádu 3, v každém homomorfismu $f : \mathbb{S}_3 \to \mathbb{Z}_4$ se každá z permutací $(1,2,3)$ a $(1,3,2)$ zobrazí na $[0]_4$. Permutace $(1,2)$ se může zobrazit jen na prvek řádu 1 nebo 2, tj. na $[0]_4$ nebo $[2]_4$. Protože $(1,2) \circ (1,2,3) = (2,3)$ a $(1,2,3) \circ (1,2) = (1,3)$, platí

$$f((2,3)) \;=\; f((1,2)) + f((1,2,3)) \;=\; f((1,2)) + [0]_4 \;=\; f((1,2)),$$
$$f((1,3)) \;=\; f((1,2,3)) + f((1,2)) \;=\; [0]_4 + f((1,2)) \;=\; f((1,2)).$$

Máme tedy dvě možnosti, jak definovat f: v prvním případě se každý prvek grupy $\mathbb{S}_3$ zobrazí na $[0]_4$, zřejmě to je homomorfismus a jeho jádro je $\mathbb{S}_3$. Ve druhém případě se každá transpozice zobrazí na $[2]_4$ a ostatní prvky na $[0]_4$. Protože liché permutace jsou zobrazeny na $[2]_4$ a sudé permutace na $[0]_4$, jde také o homomorfismus, jeho jádro je množina $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

Izomorfní grupy

Definice. Řekneme, že grupy G_1 a G_2 jsou **izomorfní**, a píšeme $G_1 \cong G_2$, jestliže existuje alespoň jeden izomorfismus $f : G_1 \to G_2$.

Příklad. Grupy $(\mathbb{R}^+, \cdot)$ a $(\mathbb{R}, +)$ jsou izomorfní, neboť logaritmus $\log : \mathbb{R}^+ \to \mathbb{R}$ je izomorfismus.

Věta. *Jsou-li G_1, G_2, G_3 grupy. Pak platí*

- $G_1 \cong G_1$,
- $G_1 \cong G_2 \implies G_2 \cong G_1$,
- $G_1 \cong G_2,\ G_2 \cong G_3 \implies G_1 \cong G_3$.

[Identita na množině G_1 je izomorfismus. Inverzní zobrazení k izomorfismu je izomorfismus.

Složení dvou izomorfismů je izomorfismus.]

Věta. *Libovolná nekonečná cyklická grupa je izomorfní s grupou $(\mathbb{Z}, +)$. Libovolná konečná cyklická grupa řádu n je izomorfní s grupou $(\mathbb{Z}_n, +)$.* [Věta 6.6, str. 34]

Levé třídy rozkladu grupy podle podgrupy

Definice. Nechť $(G, \cdot)$ je grupa, H její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou **levou třídu** $a \cdot H$ rozkladu grupy G podle podgrupy H předpisem $a \cdot H = \{a \cdot h;\ h \in H\}$.

Poznámka. Podle definice je levá třída $a \cdot H$ podmnožinou grupy G, je to množina všech součinů pevně zvoleného prvku a postupně se všemi prvky $h \in H$.

Věta. *Nechť $(G, \cdot)$ je grupa, H její podgrupa, $a, b \in G$ libovolné. Následující podmínky jsou ekvivalentní:*

- $a \cdot H = b \cdot H$,
- $a \in b \cdot H$,
- $b^{-1} \cdot a \in H$.

[Věta 7.2, str. 37]

Označení. Označme G/H množinu všech levých tříd grupy G podle podgrupy H, tj. $G/H = \{a \cdot H;\ a \in G\}$.

Rozklad grupy podle podgrupy

Příklad. Pro libovolné $m \in \mathbb{N}$ tvoří množina H všech celých čísel dělitelných číslem m podgrupu grupy $(\mathbb{Z}, +)$ a platí $\mathbb{Z}/H = \mathbb{Z}_m$.

[Platí $H = \{mk;\ k \in \mathbb{Z}\}$ a pro každé $a \in \mathbb{Z}$ je $a + H = \{a + mk;\ k \in \mathbb{Z}\} = [a]_m$.]

Příklad. Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = H$, $(1,3) \circ H = \{(1,3) \circ \mathrm{id}, (1,3) \circ (1,2)\} = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = \{(2,3) \circ \mathrm{id}, (2,3) \circ (1,2)\} = \{(2,3), (1,3,2)\}$, a tedy $G/H = \big\{H, \{(1,3), (1,2,3)\}, \{(2,3), (1,3,2)\}\big\}$.

Poznámka. Připomeňme, že rozkladem na množině M rozumíme systém neprázdných podmnožin množiny M, jejichž sjednocení je rovno celé množině M a které jsou po dvou disjunktní.

Věta. *Množina G/H všech levých tříd grupy G podle podgrupy H tvoří rozklad na množině G.* [Věta 7.2, str. 37]

Definice. Počet $|G/H|$ všech levých tříd grupy G podle podgrupy H se nazývá **index** podgrupy H v grupě G.

Věta. *Nechť $(G, \cdot)$ je konečná grupa, H její podgrupa. Pak platí $|G| = |G/H| \cdot |H|$.* [Věta 7.6, str. 38]

Lagrangeova věta a její důsledky

Věta. *Nechť $(G, \cdot)$ je konečná grupa, H její podgrupa. Pak platí $|G| = |G/H| \cdot |H|$.*

Důsledek (Lagrangeova věta). *Řád libovolné podgrupy konečné grupy G je dělitelem řádu grupy G.*

Důsledek. *Řád libovolného prvku konečné grupy G je dělitelem řádu grupy G.* [Řád libovolného $a \in G$ je roven řádu podgrupy $\langle a \rangle$, kterou generuje.]

Důsledek. *Libovolná grupa prvočíselného řádu je cyklická.* [Důsledek 7.9, str. 39]

Důsledek. *Nechť G je konečná grupa řádu $n = |G|$. Pak pro libovolný prvek $a \in G$ platí $a^n = 1$. Jinými slovy: exponent konečné grupy G je dělitelem řádu grupy G.*

Speciálním případem předchozího důsledku je následující věta z teorie čísel:

Věta (Eulerova). *Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$ jsou libovolná nesoudělná čísla. Pak platí $a^{\varphi(m)} \equiv 1 \pmod{m}$.* [Věta 7.11, str. 39]

Naivní pokus o zavedení operace na rozkladu G/H

Inspirace. Zvolme pevně libovolné $m \in \mathbb{N}$ a jako dříve označme $H = [0]_m = \{mk;\ k \in \mathbb{Z}\}$. Pak H je podgrupa grupy $(\mathbb{Z}, +)$ a odpovídajícím rozkladem je $\mathbb{Z}/H = \mathbb{Z}_m$. Na $\mathbb{Z}_m$ jsme definovali operaci $+$ pomocí reprezentantů: pro libovolné $a \in \mathbb{Z}$ je totiž $a + H = [a]_m$ a použitou definici sčítání zbytkových tříd $[a]_m + [b]_m = [a + b]_m$ pro libovolná $a, b \in \mathbb{Z}$ lze psát ve tvaru $(a + H) + (b + H) = (a + b) + H$.

Pokus o zobecnění. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pak bychom na rozkladu G/H rádi zavedli operaci $\cdot$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ pro libovolná $a, b \in G$. Je to ale vždy možné?

Příklad. Pro $G = \mathbb{S}_3$ a $H = \{\mathrm{id}, (1,2)\}$ je $\mathrm{id} \circ H = (1,2) \circ H = H$, $(1,3) \circ H = (1,2,3) \circ H = \{(1,3), (1,2,3)\}$ a $(2,3) \circ H = (1,3,2) \circ H = \{(2,3), (1,3,2)\}$, a tedy předchozí definice pomocí reprezentantů by dala $(1,3,2) \circ H = \big((1,2) \circ H\big) \circ \big((1,3) \circ H\big) = \big(\mathrm{id} \circ H\big) \circ \big((1,3) \circ H\big) = (1,3) \circ H$, což však není pravda.

Normální podgrupy

Úvaha. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Pro libovolné $h \in H$ platí $h \cdot H = 1 \cdot H$, a tedy pro každé $a \in G$ musí operace $\cdot$ na G/H splňovat $(h \cdot H) \cdot (a^{-1} \cdot H) = (1 \cdot H) \cdot (a^{-1} \cdot H)$. Abychom mohli zavést operaci pomocí reprezentantů, muselo by platit $(h \cdot a^{-1}) \cdot H = a^{-1} \cdot H$, neboli $a \cdot h \cdot a^{-1} \in H$.

Definice. Nechť $(G, \cdot)$ je grupa a H její podgrupa. Řekneme, že H je **normální podgrupou** grupy G, jestliže pro každé $h \in H$ a každé $a \in G$ platí $a \cdot h \cdot a^{-1} \in H$.

Příklad. V každé grupě G jsou $\{1\}$ i G normální podgrupy. Podgrupa $H = \{\mathrm{id}, (1,2)\}$ není normální podgrupou grupy $\mathbb{S}_3$.

Věta. *V komutativní grupě G je každá podgrupa normální.*

Věta. *Je-li $f : G \to K$ homomorfismus grup, pak jeho jádro* $\ker f$ *je normální podgrupa grupy G.* [Víme, že $\ker f$ je pogrupa. Je-li $h \in \ker f$, tj. $f(h) = 1$, pak pro každé $a \in G$ je $f(a \cdot h \cdot a^{-1}) = f(a) \cdot f(h) \cdot f(a)^{-1} = 1$, proto $a \cdot h \cdot a^{-1} \in \ker f$.]

Normální podgrupy - přehledné zopakování

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Pokud má být možné na rozkladu G/H zavést operaci pomocí reprezentantů, tj. pro libovolné $a, b \in G$ definovat **součin levých tříd** $a \cdot H$ a $b \cdot H$ předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$, pak musí podgrupa H být **normální podgrupa** grupy G, tj. pro každé $h \in H$ a každé $a \in G$ musí platit $a \cdot h \cdot a^{-1} \in H$.

Ukážeme si, že pokud H je normální podgrupa grupy G, pak tímto předpisem operace na rozkladu G/H skutečně vznikne.
Dokonce platí, že G/H s touto operací tvoří grupu.

Faktorgrupa

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa.* [Věta 9.4, str. 46]

Definice. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Grupa G/H z předchozí věty se nazývá **faktorová grupa** grupy G podle (normální) podgrupy H, zkráceně **faktorgrupa**.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Zobrazení $\pi : G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro $\ker \pi = H$.* [Věta 9.5, str. 46]

Definice. Toto π se nazývá **projekce grupy G na faktorgrupu G/H**.

Důsledek. *Normální podgrupy grupy G jsou právě jádra homomorfismů $G \to K$ grupy G do vhodných grup K.*

Věta. *Nechť $(G, \cdot)$ je komutativní grupa, pak je každá podgrupa H grupy G normální a faktorgrupa G/H je komutativní.* [Věta 9.8, str. 47]

Rozklad grupy podle jádra homomorfismu

Věta. *Nechť* $f : G \to K$ *je homomorfismus grup,* $\ker f$ *jeho jádro. Pak pro libovolné* $a, b \in G$ *platí* $f(a) = f(b)$, *právě když* $a^{-1} \cdot b \in \ker f$, *tj. právě když* $a \cdot (\ker f) = b \cdot (\ker f)$.

Důkaz. Víme, že pro libovolnou podgrupu H grupy G platí
$a^{-1} \cdot b \in H \quad \Leftrightarrow \quad a \cdot H = b \cdot H$,
proto to platí i pro $H = \ker f$.

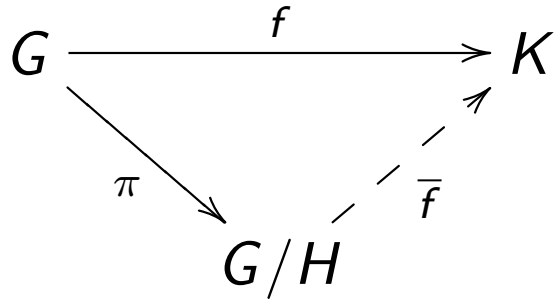
Jestliže platí $f(a) = f(b)$, pak
$f(a^{-1} \cdot b) = f(a^{-1}) \cdot f(b) = f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(1) = 1$,
a tedy $a^{-1} \cdot b \in \ker f$.

Jestliže naopak platí $a^{-1} \cdot b \in \ker f$, pak $f(a^{-1} \cdot b) = 1$, proto
$f(a) = f(a) \cdot 1 = f(a) \cdot f(a^{-1} \cdot b) = f(a \cdot a^{-1} \cdot b) = f(b)$.

Úvaha

Předpokládejme, že je dán homomorfismus grup $f : G \to K$.
Navíc mějme dánu normální podgrupu H grupy G.
Pak máme faktorgrupu G/H a projekci $\pi : G \to G/H$.
Chceme vědět, jestli existuje zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

To můžeme znázornit diagramem takto:

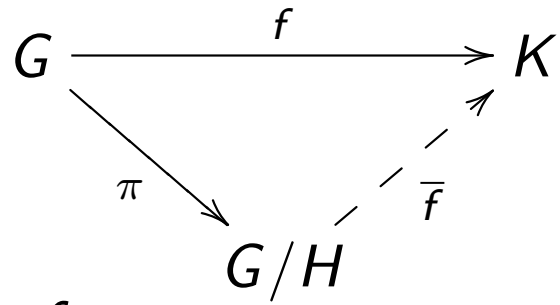


Pro každý prvek $h \in H$ platí $\pi(h) = h \cdot H = 1 \cdot H = \pi(1)$.

Pokud takové $\overline{f}$ existuje, musí pro každý prvek $h \in H$ platit
$f(h) = (\overline{f} \circ \pi)(h) = \overline{f}(\pi(h)) = \overline{f}(\pi(1)) = (\overline{f} \circ \pi)(1) = f(1) = 1$,
a tedy $h \in \ker f$.
Pokud tedy není splněna podmínka $H \subseteq \ker f$, nemůže takové $\overline{f}$ existovat.
Ale stačí tato podmínka, aby byla existence $\overline{f}$ zaručena?

Hlavní věta o faktorových grupách

Věta (Hlavní věta o faktorových grupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H. Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.*



Navíc platí:

- *$\overline{f}$ je homomorfismus grup,*
- *$\overline{f}$ je injekce, právě když $H = \ker f$,*
- *$\overline{f}$ je surjekce, právě když f je surjekce.*

Důkaz. Libovolný prvek G/H je tvaru $a \cdot H = \pi(a)$ pro vhodné $a \in G$. Pak pro libovolné zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$ musí platit $\overline{f}(a \cdot H) = \overline{f}(\pi(a)) = (\overline{f} \circ \pi)(a) = f(a)$. Jediná možnost, jak definovat $\overline{f}$, je předpisem $\overline{f}(a \cdot H) = f(a)$. Ale $a \cdot H = b \cdot H \Leftrightarrow a^{-1} \cdot b \in H \Rightarrow a^{-1} \cdot b \in \ker f \Leftrightarrow f(a) = f(b)$. Odtud nejen korektnost definice $\overline{f}$, ale také $H = \ker f \Leftrightarrow \overline{f}$ injekce. Dále $\{\overline{f}(a \cdot H);\ a \in G\} = \{f(a);\ a \in G\}$, tj. f surjekce $\Leftrightarrow \overline{f}$ surjekce.

Rozklad grupy podle jádra homomorfismu podruhé

Důsledek. *Je-li* $f : G \to K$ *surjektivní homomorfismus grup, pak platí* $G/(\ker f) \cong K$.

Důsledek. *Je-li* $f : G \to K$ *homomorfismus grup, pak platí* $G/(\ker f) \cong f(G)$, *kde* $f(G) = \{f(a);\, a \in G\} \subset K$ *je obraz* G.

Příklad. Pro libovolnou grupu G je $\mathrm{id} : G \to G$ homomorfismus s jádrem $\ker \mathrm{id} = \{1\}$, proto $G/\{1\} \cong G$. Přitom $G/\{1\} = \{\{a\};\, a \in G\}$ a v tomto izomorfismu $\{a\} \mapsto a$.

Příklad. Zobrazení $\mathrm{sgn} : \mathbb{R}^* \to \{1, -1\}$, které zobrazí kladná čísla na 1 a záporná na -1, je homomorfismus. Platí $\ker \mathrm{sgn} = \mathbb{R}^+$, proto $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\} \cong \{1, -1\}$, přičemž $\mathbb{R}^+ \mapsto 1$, $\mathbb{R}^- \mapsto -1$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{R}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{R}^*$, je homomorfismus grupy $(\mathbb{R}^*, \cdot)$ do sebe s jádrem $\ker \mathrm{abs} = \{1, -1\}$ a obrazem $\mathrm{abs}(\mathbb{R}^*) = \mathbb{R}^+$, proto faktorgrupa $(\mathbb{R}^*/\{1, -1\}, \cdot) \cong (\mathbb{R}^+, \cdot)$. Zde třída $\{a, -a\} \mapsto |a|$.

Další příklady

Příklad. Nechť $n \in \mathbb{N}$, $n > 1$. Zobrazení parity $p : \mathbb{S}_n \to \{1, -1\}$ je surjektivní homomorfismus grup, jehož jádrem je normální podgrupa všech sudých permutací $\mathbb{A}_n = \ker p$, proto faktorgrupa $(\mathbb{S}_n/\mathbb{A}_n, \circ) \cong (\{1, -1\}, \cdot)$.

Příklad. Zobrazení $f : \mathbb{R} \to \mathbb{C}^*$ s předpisem $f(x) = \cos x + i \sin x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{C}^*, \cdot)$, neboť platí $\cos(x + y) + i \sin(x + y) = (\cos x + i \sin x) \cdot (\cos y + i \sin y)$ pro libovolné $x, y \in \mathbb{R}$. Jádrem je podgrupa $\ker f = \{2k\pi;\ k \in \mathbb{Z}\}$ všech celočíselných násobků 2π. Obrazem $f(\mathbb{R}) = \{\cos x + i \sin x;\ x \in \mathbb{R}\} = \{a \in \mathbb{C};\ |a| = 1\}$ je podgrupa všech komplexních čísel s absolutní hodnotou 1. Proto $(\mathbb{R}/\{2k\pi;\ k \in \mathbb{Z}\}, +) \cong (\{a \in \mathbb{C};\ |a| = 1\}, \cdot)$.

Příklad. Zobrazení $\mathrm{abs} : \mathbb{C}^* \to \mathbb{R}^*$, určené předpisem $\mathrm{abs}(x) = |x|$ pro každé $x \in \mathbb{C}^*$, je homorfismus grupy $(\mathbb{C}^*, \cdot)$ do grupy $(\mathbb{R}^*, \cdot)$ s jádrem $\ker \mathrm{abs} = \{a \in \mathbb{C};\ |a| = 1\}$ a obrazem $\mathrm{abs}(\mathbb{C}^*) = \mathbb{R}^+$, proto faktorgrupa $(\mathbb{C}^*/\{a \in \mathbb{C};\ |a| = 1\}, \cdot) \cong (\mathbb{R}^+, \cdot)$.

Součin grup

Věta. *Nechť* $(G_1, \cdot)$ *a* $(G_2, \cdot)$ *jsou grupy. Definujme na kartézském součinu* $G_1 \times G_2$ *novou operaci* $\cdot$ *po složkách, tj. definujeme* $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \cdot h_1, g_2 \cdot h_2)$ *pro libovolné* $g_1, h_1 \in G_1$ *a* $g_2, h_2 \in G_2$. *Pak* $(G_1 \times G_2, \cdot)$ *je grupa.* [Věta 6.7, str. 35]

Definice. Výše popsaná grupa $(G_1 \times G_2, \cdot)$ se nazývá **součin grup** $(G_1, \cdot)$ a $(G_2, \cdot)$. Zobrazení

$$p_1 : G_1 \times G_2 \to G_1 \qquad \text{a} \qquad p_2 : G_1 \times G_2 \to G_2$$

určená předpisy

$$p_1((a, b)) = a, \qquad p_2((a, b)) = b$$

pro libovolné $(a, b) \in G_1 \times G_2$ se nazývají **projekce** (ze součinu).

Věta. *Nechť* $(G_1 \times G_2, \cdot)$ je součin grup $(G_1, \cdot)$ a $(G_2, \cdot)$. Pak obě projekce p_1 a p_2 jsou surjektivní homomorfismy. [Věta 8.12, str. 43]

Cayleyho věta

Věta. *Nechť $(G, \cdot)$ je grupa, zvolme libovolně $a \in G$. Pak zobrazení $r_a : G \to G$, určené předpisem $r_a(g) = a \cdot g$ pro každé $g \in G$, je bijekce, tedy $r_a \in \mathbb{S}(G)$.* [Věta 4.18, str. 28]

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme bijekci r_a z předchozí věty. Vznikne tak zobrazení $r : G \to \mathbb{S}(G)$ s předpisem $r(a) = r_a$ pro každé $a \in G$. Pak platí: r je injektivní homomorfismus grup.* [Věta 8.13, str. 43]

Důsledek (Cayleyho věta). *Každá grupa G je izomorfní s vhodnou podgrupou grupy permutací $\mathbb{S}(G)$. Každá konečná grupa řádu n je izomorfní s vhodnou podgrupou grupy $\mathbb{S}_n$.* [Věta 8.14, str. 43]

Poznámka. V předchozí větě jsme každý prvek a grupy $(G, \cdot)$ reprezentovali permutací r_a nosné množiny G. Tuto situaci lze zobecnit, můžeme prvky grupy $(G, \cdot)$ reprezentovat permutacemi nějaké jiné množiny X, kterou můžeme libovolně zvolit. Budeme tedy studovat homomorfismy $G \to \mathbb{S}(X)$. Této situaci říkáme reprezentace grupy G permutacemi na množině X anebo stručně **akce grupy G na množině X**.

Akce grupy G na množině X

Definice. Nechť G je grupa, X množina a $\varphi : G \to \mathbb{S}(X)$ je homomorfismus grup. Pro libovolné $a \in G$ je $\varphi(a) \in \mathbb{S}(X)$, je tedy $\varphi(a) : X \to X$ bijekce. V bijekci $\varphi(a)$ máme pro každý prvek $y \in X$ dán jeho obraz $\varphi(a)(y) \in X$. Pro libovolné $y \in X$ se množina $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ nazývá **stabilizátor** prvku y, množina $O_y = \{\varphi(a)(y);\ a \in G\} \subseteq X$ **orbita** prvku y (vzhledem k φ).

Příklad. Zvolme $n \in \mathbb{N}$ a $X = \{1, 2, \ldots, n\}$. Pak $\mathbb{S}(X) = \mathbb{S}_n$. Zvolme dále libovolně $f \in \mathbb{S}_n$ a označme $G = \langle f \rangle$, tj. G je podgrupa grupy $\mathbb{S}_n$ generovaná permutací f. Potom φ lze zvolit jako inkluzi, tj. každý prvek grupy G je zobrazen na sebe. Pokud zapíšeme permutaci f jako složení nezávislých cyklů, ihned vidíme, jak vypadá orbita O_y pro libovolný $y \in X$: platí-li $f(y) = y$, je $O_y = \{y\}$, v opačném případě je O_y množina všech prvků z cyklu, v němž vystupuje y. Stabilizátorem S_y prvku y je množina všech mocnin f^k permutace f, které ponechávají y na místě, tj. splňují $f^k(y) = y$. Jde o podgrupu grupy G generovanou permutací $f^{|O_y|}$, tj. $S_y = \langle f^{|O_y|} \rangle$. Platí proto $|G/S_y| = |O_y|$.

Akce grupy G na množině X

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta. *Množina všech orbit $\{O_y;\ y \in X\}$ je rozklad na množině X.*

[Věta 8.17, str. 44]

Věta. *Pro libovolné $y \in X$ tvoří stabilizátor S_y podgrupu grupy G.*

Věta. *Předpokládejme navíc, že X je konečná množina. Pak pro každé $y \in X$ je počet prvků v orbitě O_y roven indexu stabilizátoru S_y, tj. $|O_y| = |G/S_y|$.* [Věta 8.19, str. 45]

Důsledek. *Nechť je navíc X konečná množina a $y_1, \ldots, y_m \in X$ jsou takové, že v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$ (a tedy m je počet orbit). Pak platí $|X| = \sum_{i=1}^{m} |G/S_{y_i}|$.* [Důsledek 8.20, str. 45]

Věta (Burnsidovo lemma). *Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.*

Důkaz Burnsidova lemmatu

Mějme dáno: grupu G, množinu X a homomorfismus grup $\varphi : G \to \mathbb{S}(X)$, určující pro libovolný prvek $y \in X$ stabilizátor $S_y = \{a \in G;\ \varphi(a)(y) = y\}$ a orbitu $O_y = \{\varphi(a)(y);\ a \in G\}$.

Věta (Burnsidovo lemma). Nechť je navíc G konečná grupa a X konečná množina. Pro libovolné $a \in G$ nechť F_a je množina fixních bodů permutace $\varphi(a)$, tedy $F_a = \{y \in X;\ \varphi(a)(y) = y\}$. Pak pro počet orbit platí $m = \frac{1}{|G|} \sum_{a \in G} |F_a|$.

Důkaz. Nechť v každé orbitě leží právě jeden z prvků $y_1, \ldots, y_m$.

$$\sum_{a \in G} |F_a| = \left|\{(a, y) \in G \times X;\ \varphi(a)(y) = y\}\right| = \sum_{y \in X} |S_y| =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} |S_y| = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|G/S_y|} = \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_y|} =$$

$$= \sum_{i=1}^{m} \sum_{y \in O_{y_i}} \frac{|G|}{|O_{y_i}|} = \sum_{i=1}^{m} |O_{y_i}| \frac{|G|}{|O_{y_i}|} = \sum_{i=1}^{m} |G| = m|G|.$$

Příklad užití Burnsidova lemmatu v kombinatorice

Příklad. Máme stejné korálky n různých barev. Děláme dětské náramky tak, že navlečeme 7 korálků na šňůrku a zavážeme. Kolik různých náramků lze takto vytvořit (poloha uzlíku nerozhoduje)?

Řešení. Pro $n = 1$ je jediný, pro $n = 2$ lze promyslet, že jich je 18. Ale pro $n > 2$ už naivní metodou nakreslení všech možností neuspějeme. Užijme Burnsidovo lemma, kde X je množina všech obarvení vrcholů pravidelného 7úhelníka n barvami. Pak $|X| = n^7$, každé obarvení určí náramek, ale různá obarvení mohou dát týž náramek. Abychom zjistili, která obarvení dávají stejný náramek, užijme grupu $\mathbb{D}_7$ všech symetrií pravidelného 7úhelníka a definujme $\varphi : \mathbb{D}_7 \to \mathbb{S}(X)$ takto: pro symetrii $a \in \mathbb{D}_7$ a obarvení $y \in X$ je $\varphi(a)(y)$ to obarvení, které z y vznikne, aplikujeme-li na 7úhelník symetrii a. Pak dvě obarvení z množiny X odpovídají témuž náramku, právě když patří do stejné orbity. Pro identitu id je $|F_{\mathrm{id}}| = |X| = n^7$, pro libovolnou ze 6 zbylých rotací $r \in \mathbb{D}_7$ je $|F_r| = n$ a pro každou ze 7 osových souměrností s je $|F_s| = n^4$. Podle Burnsidova lemmatu je hledaný počet $\frac{1}{14}(n^7 + 7n^4 + 6n)$.

Vnitřní izomorfismy grupy G

Věta. *Nechť $(G, \cdot)$ je grupa. Pro libovolné $a \in G$ definujme zobrazení $\rho_a : G \to G$ předpisem $\rho_a(g) = a \cdot g \cdot a^{-1}$ pro každé $g \in G$. Pak pro každé $a, b \in G$ je $\rho_a \circ \rho_b = \rho_{ab}$. Navíc je ρ_a izomorfismus a platí $\rho_a^{-1} = \rho_{a^{-1}}$.*

Důkaz. Pro libovolné $a, b, g \in G$ platí $(\rho_a \circ \rho_b)(g) = \rho_a(\rho_b(g)) = \rho_a(b \cdot g \cdot b^{-1}) = a \cdot b \cdot g \cdot b^{-1} \cdot a^{-1} = (a \cdot b) \cdot g \cdot (a \cdot b)^{-1} = \rho_{ab}(g)$.

Zřejmě $\rho_1(g) = 1 \cdot g \cdot 1^{-1} = g = \mathrm{id}(g)$, a tedy $\rho_1 = \mathrm{id}$.

Odtud plyne, že $\rho_a \circ \rho_{a^{-1}} = \mathrm{id}$ a $\rho_{a^{-1}} \circ \rho_a = \mathrm{id}$, tedy ρ_a je bijekce a platí $\rho_a^{-1} = \rho_{a^{-1}}$.

Konečně pro libovolné $a, g, h \in G$ platí $\rho_a(g) \cdot \rho_a(h) = a \cdot g \cdot a^{-1} \cdot a \cdot h \cdot a^{-1} = a \cdot g \cdot h \cdot a^{-1} = \rho_a(g \cdot h)$, je tedy ρ_a homomorfismus.

Definice. Izomorfismy z předchozí věty nazýváme vnitřní izomorfismy grupy G.

Akce grupy G na množině G vnitřními izomorfismy

Definice. Nechť $(G, \cdot)$ je grupa. Jejím centrem $Z(G)$ rozumíme množinu všech prvků, které komutují s každým prvkem grupy G, tj. $Z(G) = \{a \in G;\ \forall g \in G : a \cdot g = g \cdot a\}$.

Věta. *Nechť $(G, \cdot)$ je grupa. Libovolnému prvku $a \in G$ přiřaďme vnitřní izomorfismus ρ_a z předchozí věty. Vznikne tak zobrazení $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$. Pak platí: ρ je homomorfismus grup, udává tedy akci grupy G na nosné množině G této grupy. Přitom jádro $\ker \rho = Z(G)$. Pro libovolný prvek $g \in G$ platí, že g má jednoprvkovou orbitu v této akci, právě když g je v centru grupy G, tj. $O_g = \{g\} \quad \Leftrightarrow \quad g \in Z(G)$.*

Důsledek. *Centrum $Z(G)$ je normální podgrupa grupy G. Obraz $\rho(G)$ grupy G v homomorfismu ρ je izomorfní s faktorgrupou $G/Z(G)$. Grupa G má tedy právě $\frac{|G|}{|Z(G)|}$ vnitřních izomorfismů.*

Poznámka. Je-li H podgrupa grupy G taková, že $H \subseteq Z(G)$, pak H je normální podgrupa grupy G. [$\forall a \in G\ \forall h \in H$: $a \cdot h \cdot a^{-1} = h \cdot a \cdot a^{-1} = h \in H$.]

Užití předchozí akce na p-grupách

Definice. Nechť p je prvočíslo. Konečná grupa G se nazývá **p-grupa**, jestliže $|G| = p^k$ pro vhodné $k \in \mathbb{N}$.

Věta. Nechť p je prvočíslo a G je p-grupa. Pak $|Z(G)| > 1$, tj. G má netriviální centrum.

Důkaz. Platí $|G| = p^k$ pro nějaké $k \in \mathbb{N}$. Užijeme výše popsanou akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a) = \rho_a$ pro každé $a \in G$.
Víme: počet prvků libovolné orbity je index stabilizátoru, tento index je dělitelem řádu grupy G, tj. čísla $|G| = p^k$. Dále platí

$$\begin{aligned} a \in Z(G) \quad &\Leftrightarrow \quad |O_a| = 1, \\ a \notin Z(G) \quad &\Rightarrow \quad p \mid |O_a|. \end{aligned}$$

Každý prvek z G patří do právě jedné orbity, počet prvků grupy $|G|$ je dělitelný číslem p. Sečtením právě $|Z(G)|$ jedniček a několika sčítanců dělitelných p dostaneme součet dělitelný p. Proto je počet těchto jedniček dělitelný p, tedy $p \mid |Z(G)|$.

Konečné grupy

Věta. *Nechť p je prvočíslo a G je p-grupa řádu $|G| = p^2$. Pak je G komutativní.*

Důkaz. Podle Lagrangeovy věty a předchozí věty je $|Z(G)|$ dělitel p^2 větší než 1. Pokud $|Z(G)| = p^2$, je $G = Z(G)$ komutativní. Předpokládejme tedy $|Z(G)| = p$ a dojděme ke sporu. Pak existuje $a \in G - Z(G)$, a tedy $M = Z(G) \cup \{a, a^{-1}\}$ má více než p prvků, proto podle Lagrangeovy věty $\langle M \rangle = G$. Ovšem podle věty o podgrupě generované množinou je libovolný prvek $\langle M \rangle$ součinem několika prvků z M. Protože prvky z centra $Z(G)$ komutují s každým prvkem grupy G, je

$$G = \langle M \rangle = \{a^n \cdot h \mid n \in \mathbb{Z}, h \in Z(G)\}.$$

Pro libovolná $h, h' \in Z(G)$ a $n, n' \in \mathbb{Z}$ pak platí $(a^n \cdot h) \cdot (a^{n'} \cdot h') = a^{n+n'} \cdot h \cdot h' = (a^{n'} \cdot h') \cdot (a^n \cdot h)$. Je tedy grupa G komutativní, tudíž $Z(G) = G$, spor.

Důsledek. *Nechť p je prvočíslo. Pak existují, až na izomorfismus, právě dvě grupy řádu p^2, a sice $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Důkaz. Nechť G je grupa řádu p^2. Pokud v G existuje prvek řádu p^2, je G cyklická a platí $G \cong \mathbb{Z}_{p^2}$. Předpokládejme tedy, že v G žádný prvek řádu p^2 neexistuje. Zvolme libovolně $a \in G$, $a \neq 1$. Pak řád prvku a je p. Zvolme libovolně $b \in G - \langle a \rangle$. Rovněž řád prvku b je p. Nechť zobrazení $f : \mathbb{Z}_p \times \mathbb{Z}_p \to G$ je určené předpisem $f(([n]_p, [m]_p)) = a^n \cdot b^m$. Protože řády obou prvků a, b jsou p, je toto zobrazení definováno korektně.
Protože G je komutativní, je f homomorfismus grup. Přitom obraz $f(\mathbb{Z}_p \times \mathbb{Z}_p)$ obsahuje všechny mocniny prvku a i prvek b, je to tedy podgrupa grupy G mající více než p prvků, tedy f je surjektivní. Protože $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2 = |G|$, je f bijekce, tudíž izomorfismus.

Motivace následujících vět

Poznámka. Pro libovolnou konečnou grupu G nám Lagrangeova věta říká, že řád každé podgrupy grupy G dělí řád grupy G.
Naopak se můžeme ptát, jestli pro každého dělitele d řádu grupy G existuje podgrupa H grupy G mající řád d.
Takto obecně to pravda není, je možné ukázat, že například grupa $\mathbb{A}_4$ řádu 12 nemá žádnou podgrupu řádu 6.
Pomocí akce grupy na množině v následujících větách ukážeme, že to je pravda, pokud je d mocnina prvočísla.

Cauchyho věta

Věta (Cauchy). Nechť G je konečná grupa a p prvočíslo dělící řád grupy G. Pak G obsahuje alespoň jednu podgrupu řádu p.

Důkaz. Označme
$X = \{(y_1, \ldots, y_p) \mid y_1, \ldots, y_p \in G,\ y_1 \ldots y_p = 1\}$.
Zřejmě $|X| = |G|^{p-1}$ je dělitelné p. Definujme $\alpha \in \mathbb{S}(X)$ předpisem $\alpha((y_1, \ldots, y_p)) = (y_2, \ldots, y_p, y_1)$. Pak $\alpha^p = \mathrm{id}$, a tedy máme homomorfismus $\varphi : \mathbb{Z}_p \to \mathbb{S}(X)$ určený předpisem $\varphi([n]_p) = \alpha^n$. Je tedy dána akce grupy $\mathbb{Z}_p$ na X. Pro libovolné $x = (y_1, \ldots, y_p) \in X$ orbita O_x má jediný prvek, je-li $y_1 = \cdots = y_p$, a právě p prvků jinak. Protože orbity tvoří rozklad množiny X, je $|X|$ součtem několika sčítanců, z nichž každý je 1 nebo p. Přitom počet jedniček je dělitelný p a alespoň jedna jednička tam je: máme orbitu $\{(1, \ldots, 1)\}$. Proto existuje orbita $\{(g, \ldots, g)\}$ pro nějaké $g \in G$, $g \neq 1$. Pak řád g je roven p a $\langle g \rangle$ je hledaná p-prvková podgrupa grupy G.

První Sylowova věta

Následující věta je zobecněním Cauchyho věty:

Věta (Sylow). Nechť G je konečná grupa řádu n. Nechť p je prvočíslo a $k \in \mathbb{N}$ takové, že $p^k \mid n$. Pak G obsahuje alespoň jednu podgrupu řádu p^k.

Důkaz provedeme indukcí vzhledem k n. Pro $n = 1$ věta platí (takové p neexistuje).
Nechť $n > 1$ a pro grupy řádu menšího než n věta platí.
Rozlišíme dva případy, nejprve předpokládejme, že $p \mid |Z(G)|$.
Podle Cauchyho věty existuje podgrupa $H \subseteq Z(G)$ řádu p. Pak H je normální podgrupa grupy G, faktorgrupa G/H má $\frac{n}{p} < n$ prvků, a tedy pro ni platí indukční předpoklad. Protože $p^{k-1} \mid \frac{n}{p}$, existuje podgrupa K grupy G/H řádu $|K| = p^{k-1}$. Její vzor $\pi^{-1}(K)$ v projekci $\pi : G \to G/H$ je podgrupa grupy G řádu p^k.

Pokračování důkazu první Sylowovy věty

Předpokládejme naopak, že $p \nmid |Z(G)|$. Užijme znovu akci $\rho : G \to \mathbb{S}(G)$ s předpisem $\rho(a)(g) = a \cdot g \cdot a^{-1}$. Víme, že jednoprvkové orbity mají právě prvky z centra. Protože orbity tvoří rozklad množiny G, platí

$$|G| = |Z(G)| + t_1 + \cdots + t_r,$$

kde $t_1 > 1, \ldots, t_r > 1$ jsou počty prvků v orbitách. Víme, že $p \mid |G|$ a $p \nmid |Z(G)|$, existuje tedy i tak, že $p \nmid t_i$. Protože $t_i = |O_x|$ pro vhodné $x \in G$, je t_i index stabilizátoru S_x, tedy $|G| = |S_x| \cdot t_i$. Pak $p^k \mid |S_x|$ a $|S_x| < n$. Podle indukčního předpokladu má grupa S_x podgrupu H řádu p^k. Protože H je také podgrupa grupy G, jsme hotovi.

p-Sylowské podgrupy, druhá Sylowova věta

Definice. Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že p^k je největší mocnina p dělící řád grupy G, tj. $|G| = p^k \cdot m$, přičemž $p \nmid m$. Pak libovolná podgrupa grupy G mající řád p^k se nazývá **p-Sylowská podgrupa** grupy G (někdy též Sylowova p-podgrupa).

Příklad. Grupa $(\mathbb{S}_3, \circ)$ řádu 6 obsahuje tři 2-Sylowské podgrupy, totiž $\{\mathrm{id}, (1,2)\}$, $\{\mathrm{id}, (1,3)\}$, $\{\mathrm{id}, (2,3)\}$. Obsahuje také jedinou 3-Sylowskou podgrupu, totiž $\{\mathrm{id}, (1,2,3), (1,3,2)\}$.

Věta (Sylow). Nechť G je konečná grupa, p prvočíslo a $k \in \mathbb{N}$ takové, že $|G| = p^k \cdot m$ a $p \nmid m$. Označme r počet p-Sylowských podgrup grupy G. Pak platí

- $r \equiv 1 \pmod{p}$, $r \mid m$;
- *libovolná podgrupa grupy G, jejíž řád je mocnina p, je podgrupou některé p-Sylowské podgrupy grupy G;*
- *jestliže H, K jsou p-Sylowské podgrupy grupy G, pak existuje $g \in G$ tak, že předpis $h \mapsto g \cdot h \cdot g^{-1}$ určuje izomorfismus $H \to K$.* [První vlastnost viz [Věta 10.10, str. 51], zbytek Dummit, Foote: Abstract algebra, str. 139.]

Struktura konečných komutativních grup

Věta. Nechť $(G, \cdot)$ je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \ldots, p_s$ a $k_1, \ldots, k_s \in \mathbb{N}$ tak, že

$$(G, \cdot) \cong (\mathbb{Z}_{p_1^{k_1}}, +) \times \cdots \times (\mathbb{Z}_{p_s^{k_s}}, +).$$

Tento rozklad grupy G na součin cyklických p-grup je určen jednoznačně až na pořadí činitelů. Zřejmě platí $|G| = p_1^{k_1} \cdots p_s^{k_s}$.

[Věta 10.13, str. 52]

Příklad. Užijme větu k tomu, abychom zjistili, jak mohou vypadat komutativní grupy řádu 8. Podle předchozí věty jde o to, jakými způsoby je možné napsat 8 jako součin mocnin prvočísel: $8 = 2^3 = 2^2 \cdot 2 = 2 \cdot 2 \cdot 2$, proto každá komutativní grupa řádu 8 je izomorfní s právě jednou z grup $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Zdůrazněme, že tento výčet se týká jen komutativních grup, existují i nekomutativní grupy řádu 8, například grupa symetrií čtverce $\mathbb{D}_4$.