Grupy

Mgr. Růžena Holubová **2010**

1. Úvod

Cílem této práce je přehledně zpracovat elementární teorii algebraických struktur s jednou operací se zaměřením na teorii grup a sestavit sbírku řešených úloh, proto je práce členěna na teoretickou část a sbírku řešených příkladů.

Teoretická část obsahuje celkem sedm kapitol: Algebraické struktury s jednou operací, Základní vlastnosti grup, Cyklické grupy, Rozklady podle podgrupy, Permutační grupy, Grupy symetrií a Homomorfismy grup. Při zpracování teorie jsem čerpala nejvíce z Algebry a teoretické aritmetiky I., II. díl. Jaroslava Blažka a z Algebry Ladislava Procházky.

Sbírka příkladů je členěna na devět kapitol. Prvních sedm koresponduje s kapitolami teoretické části, osmou kapitolu představují konečné grupy, kterým jsem nechtěla v rámci teorie vyčleňovat samostatnou kapitolu. První až osmá kapitola je dále dělena do dvou podkapitol, na Řešené příklady a Příklady k procvičení. Poslední, tj. devátá kapitola, obsahuje výsledky neřešených příkladů. Při zpracování sbírky jsem vycházela zejména z těchto zdrojů: Pavel Horák: Cvičení z algebry a teoretické aritmetiky; Vít Musil: Grupy – Sbírka příkladů, bakalářská práce. Příklady, jejichž řešení jsem převzala, jsou označeny $(*)$.

2. Teoretická část

2. 1. Algebraické struktury s jednou operací

Definice 1. 1. Nechť $M \neq \emptyset$, $n \in \mathbb{N}$. Zobrazení F kartézské mocniny M^n do množiny M se nazývá *n*-ární operace (nebo též operace četnosti *n*) v množině M.
Je-li n-tice $(a_1, a_2,\ldots, a_n) \in M^n$ libovolná, pak prvek $b \in M$, který je obrazem $(a_1, a_2,\ldots, a_n)$ v zobrazení F, se nazývá výsledek operace F (aplikované na prvky $a_1, a_2,\ldots, a_n$, tzv. operandy, v tomto pořadí) a značí se $b = F(a_1, a_2,\ldots, a_n)$.

Poznámka:

1) Je-li F zobrazení z M^n do M, $F \neq \emptyset$, nazývá se parciální (částečnou) operací v M. (Operace v M se někdy nazývá úplná.)
2) Nechť $\emptyset \neq X \subseteq M$. Řekneme, že množina X je uzavřená vzhledem k operaci F, právě když pro libovolné prvky $a_1, a_2,\ldots, a_n \in X$ je $F(a_1, a_2,\ldots, a_n) \in X$.
3) Pro $n = 3$ … ternární operace … $F: M \times M \times M \to M$
   Pro $n = 2$ … binární operace … $F: M \times M \to M$
   Pro $n = 1$ … unární operace … $F: M \to M$, tj. unární operace je transformace množiny M
   Pro $n = 0$ … nulární operace … $F: M^0 \to M$; $M^0 \overset{\text{def}}{=} \{\emptyset\}$, tedy nulární operace nemá žádné operandy a jejím výsledkem je prvek množiny M

Zápis:
V případě binární operace se obvykle výsledek operace F aplikované na prvky a, b zapisuje jako $b = a_1 F a_2$ místo $b = F(a_1, a_2)$. Píšeme tedy například $b = a_1 * a_2$, $b = a_1 \circ a_2$, $b = a_1 \vartriangle a_2$, $b = a_1 + a_2$, $b = a_1 \cdot a_2$, $b = a_1 \wedge a_2$, $b = a_1 \vee a_2$, $b = a_1 \times a_2$, apod.

V dalším, pokud nebude řečeno jinak, budeme operací rozumět binární operaci.

Příklad:

- Sčítání, násobení v $\mathbb{R}$ jsou operace v $\mathbb{R}$.
- Odčítání v $\mathbb{N}$, dělení v $\mathbb{Q}$ nejsou operace v těchto množinách.
- Průnik, sjednocení, rozdíl množin jsou operace v potenci $P(M)$, $M \neq \emptyset$.
- Je-li předpis „$\circ$“ definovaný takto: $(\forall x, y \in \mathbb{Z})\ x \circ y = x - y^2$, pak „$\circ$“ je operace v $\mathbb{Z}$.

Je-li M konečná množina, lze operaci v M zadat tzv. Cayleyho tabulkou (tabulkou operace). V tabulce jsou ve svislém i vodorovném záhlaví zapsány ve stejném pořadí prvky množiny M. Do průsečíku řádku odpovídajícího prvku $x \in M$ a sloupce odpovídajícího prvku $y \in M$ je zapsán výsledek operace pro uspořádanou dvojici $(x, y) \in M^2$.

Příklad:
Nechť $M = \{m, n, p, q\}$, „$\circ$“ je operace v M definovaná Cayleyho tabulkou:

$\circ$	m	n	p	q
m	***m***	q	n	n
n	m	***n***	m	q
p	m	p	***q***	n
q	m	n	p	***p***

Z tabulky pak dostáváme:

- $m \circ m = n \circ m = p \circ m = q \circ m = n \circ p = m$
- $m \circ p = m \circ q = p \circ q = q \circ n = n$
- $p \circ n = q \circ p = q \circ q = p$
- $m \circ n = n \circ q = p \circ p = q$.

Zvýrazněna hlavní diagonála tabulky (= soubor polí, v nichž se protínají sloupce a řádky označené stejnými symboly).

Poznámka:
Z Cayleyho tabulky snadno poznáme, zda se jedná o operaci: všechna pole tabulky musí být obsazena, a to pouze prvky z dané množiny. Jsou-li některá pole prázdná, jde o parciální operaci.

Definice 1. 2. Nechť $M \neq \emptyset$. Uspořádaná dvojice (M, Ω), kde Ω je libovolná neprázdná množina operací (i různých četností) definovaných v M, se nazývá algebraická struktura (stručněji struktura). Množina M se nazývá nosič algebraické struktury (M, Ω).

Poznámka:
1) Pokud je zřejmé, jakou množinu operací Ω uvažujeme, můžeme zkráceně strukturu (M, Ω) vyjádřit jako M.
2) $(M, *)$…obecný zápis algebraické struktury s jednou (binární) operací
   $(M, +)$…aditivní zápis (pro $a, b \in M$ píšeme $a + b$ a mluvíme o součtu prvků a, b)
   $(M, \cdot)$…multiplikativní zápis (symbol „$\cdot$“ se obvykle vynechává, tedy pro $a, b \in M$ píšeme ab místo $a \cdot b$ a mluvíme o součinu prvků a, b)

Definice 1. 3. Struktura $(M, *)$ se nazývá asociativní, právě když platí:
$(\forall x, y, z \in M)\ (x * y) * z = x * (y * z)$.

Definice 1. 4. Struktura $(M, *)$ se nazývá komutativní, právě když platí:
$(\forall x, y \in M)\ x * y = y * x$.

Definice 1. 5. Struktura $(M, *)$ se nazývá struktura s neutrálním prvkem, právě když platí:
$(\exists x \in M)\ (\forall y \in M)\ x * y = y * x = y$.

Prvek x se pak nazývá neutrální prvek struktury $(M, *)$.

Poznámka:
1) V $(M, *)$ se neutrální prvek obvykle značí e, resp. n.
2) V $(M, \cdot)$ se neutrální prvek obvykle značí symbolem 1 a nazývá se jednotkový prvek, v $(M, +)$ symbolem 0 a nazývá se nulový prvek.

Lemma 1. 1. Každá struktura $(M, *)$ má nejvýše jeden neutrální prvek.
Důkaz:
- Jestliže $(M, *)$ není struktura s neutrálním prvkem, lemma platí.
- Předpokládejme, že v $(M, *)$ existují dva neutrální prvky, např. e_1, e_2. Pak pro každé $x \in M$ platí $e_1 * x = x * e_1 = x$ a současně $e_2 * x = x * e_2 = x$. Tedy $e_1 * e_2 = e_2 * e_1 = e_2$ a zároveň $e_2 * e_1 = e_1 * e_2 = e_1$, takže $e_1 = e_2$. □

Definice 1. 6. Prvek $g \in M$ se nazývá agresivní (anihilující) prvek v $(M, *)$, právě když platí:
$(\forall x \in M)\ x * g = g * x = g$.

Poznámka:
V $(M, \cdot)$ se agresivní prvek značí symbolem 0 a nazývá se nulový prvek, tedy stejně jako neutrální prvek v $(M, +)$.

Definice 1. 7. Prvek $a \in M$ se nazývá idempotentní prvek čili idempotent struktury $(M, *)$, právě když platí $a * a = a$. Struktura $(M, *)$ se nazývá idempotentní, právě když každý její prvek je idempotent.

Definice 1. 8. Struktura $(M, *)$ se nazývá struktura s inverzními prvky, právě když $(M, *)$ je struktura s neutrálním prvkem e a platí:

$$(\forall\, x \in M)\ (\exists\, y \in M)\ \ x * y = y * x = e.$$

Prvek y se pak nazývá inverzní prvek k prvku x. Prvek x se nazývá invertibilní, právě když k němu existuje aspoň jeden inverzní prvek.

Zápis:
Je-li prvek y inverzní k prvku x v obecně zadané struktuře $(M, *)$, pak píšeme $y = \overline{x}$.
V případě aditivního zápisu $(M, +)$ píšeme $y = -x$ a prvek y nazýváme opačný prvek k x (pro $a, -b \in M$ píšeme místo $a + (-b)$ pouze $a - b$).
V případě multiplikativního zápisu $(M, \cdot)$ píšeme $y = x^{-1}$ (pro $a, b^{-1} \in M$ píšeme obvykle místo ab^{-1} také $\frac{a}{b}$).

Lemma 1. 2. Je-li $(M, *)$ asociativní struktura s inverzními prvky, pak v $(M, *)$ existuje ke každému prvku právě jeden prvek inverzní.
Důkaz:
Předpokládejme, že k libovolnému prvku $x \in M$ existují dva inverzní prvky, např. y_1, y_2. Pak platí rovnost $x * y_1 = y_1 * x = e$ a zároveň $x * y_2 = y_2 * x = e$. Tedy $(y_1 * x) * y_2 = e * y_2 = y_2$ a také $(y_1 * x) * y_2 = y_1 * (x * y_2) = y_1 * e = y_1$. Odtud dostáváme $y_1 = y_2$. □

Definice 1. 9. Struktura $(M, *)$ se nazývá struktura s krácením, právě když platí:

$$(\forall\, x, y, z \in M)\ \ x * z = y * z \Longrightarrow x = y \wedge z * x = z * y \Longrightarrow x = y.$$

Pak říkáme, že v $(M, *)$ lze krátit prvkem z.

Definice 1. 10.
1) Struktura $(M, *)$ se nazývá struktura s dělením, právě když platí:

$$(\forall\, x, y \in M)\ (\exists\, z, z' \in M)\ \ x * z = y \wedge z' * x = y.$$

Pak říkáme, že struktura $(M, *)$ má vlastnost řešitelnosti základních rovnic.

2) Struktura $(M, *)$ se nazývá struktura s jednoznačným dělením, právě když platí:

$$(\forall\, x, y \in M)\ (\exists!\, z, z' \in M)\ \ x * z = y \wedge z' * x = y.$$

Lemma 1. 3. Je-li $(M, *)$ asociativní struktura s inverzními prvky, pak je strukturou s krácením.
Důkaz:

- Jsou-li $x, y, z \in M$ libovolné takové prvky, že $x * z \neq y * z$, lemma platí.
- Nechť $x, y, z \in M$ libovolné takové, že $x * z = y * z$. Protože $z \in M$, tak existuje inverzní prvek $\overline{z} \in M$ a platí $(x * z) * \overline{z} = (y * z) * \overline{z}$. Díky asociativnosti dostáváme $x * (z * \overline{z}) = y * (z * \overline{z})$, takže $x * e = y * e$, a tedy $x = y$.
- Pro $z * x = z * y$ analogicky. □

Lemma 1. 4. Jeli $(M, *)$ struktura s krácením a s dělením, pak je též s jednoznačným dělením.
Důkaz:
Nechť $x, y \in M$ libovolné. Pak existují prvky $z, z' \in M$ tak, že $x * z = y$ a současně $z' * x = y$.

- Předpokládejme, že existují $z_1, z_2 \in M$ takové, že $x * z_1 = y$ a zároveň $x * z_2 = y$. Pak $x * z_1 = x * z_2$, a tedy $z_1 = z_2$.
- Pro $z' * x = y$ analogicky. □

Lemma 1. 5. Je-li $(M, *)$ asociativní struktura s inverzními prvky, pak je strukturou s jednoznačným dělením.
Důkaz:
$(M, *)$ je asociativní struktura s inverzními prvky, proto je podle lemmatu 1. 3. s krácením, a tedy podle lemmatu 1. 4. stačí dokázat, že je strukturou s dělením.

- Nechť $x, y \in M$ libovolné a předpokládejme, že existuje $z \in M$ tak, že $x * z = y$. Protože $x \in M$, tak existuje inverzní prvek $\overline{x} \in M$ a platí $\overline{x} * (x * z) = \overline{x} * y$. Dále díky asociativnosti můžeme psát $(\overline{x} * x) * z = \overline{x} * y$, tedy $e * z = \overline{x} * y$, odkud $z = \overline{x} * y \in M$. Platí, že $x * z = x * (\overline{x} * y) = (x * \overline{x}) * y = e * y = y$. Tedy lemma platí.
- Pro $z' * x = y$ analogicky. □

Je-li M konečná množina a operace „$*$“ zadaná Cayleyho tabulkou, pak z tabulky poznáme, že struktura $(M, *)$ je

- komutativní, právě když je tabulka souměrná podle hlavní diagonály;
- s neutrálním prvkem e, právě když v tabulce existuje sloupec stejný jako svislé záhlaví a řádek stejný jako vodorovné záhlaví a sloupec i řádek jsou označeny symbolem e;
- s inverzními prvky, právě když tabulka obsahuje skupinu polí takovou, že
  - v každém řádku a v každém sloupci tabulky je aspoň jedno pole z této skupiny
  - každé pole je označeno symbolem pro neutrální prvek
  - pole jsou souměrná podle hlavní diagonály;
- s krácením, právě když se v každém řádku a v každém sloupci tabulky každý prvek z M vyskytuje nejvýše jednou;
- s dělením (jednoznačným dělením), právě když se v každém řádku a v každém sloupci tabulky každý prvek z M vyskytuje aspoň jednou (právě jednou).

Poznámka:
Asociativnost struktury $(M, *)$ z tabulky nepoznáme. V případě, že množina M má n prvků, musíme ověřit n^3 definičních vztahů $(x * y) * z = x * (y * z)$ pro každé $x, y, z \in M$. Je-li však $(M, *)$ struktura s neutrálním, resp. agresivním prvkem, pak uspořádaná trojice (x, y, z), v níž je alespoň jedna ze složek neutrální, resp. agresivní prvek, splňuje asociativnost operace „$*$“.

Příklad:
Určíme vlastnosti struktury $(M, *)$, kde $M = \{a, b, c, d\}$, operace „$*$“ je zadaná Cayleyho tabulkou:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

- M je uzavřená vzhledem k „$*$“.
- $(M, *)$ je komutativní, s neutrálním prvkem a, s inverzními prvky: $\overline{a} = a$, $\overline{b} = d$, $\overline{c} = c$, $\overline{d} = b$.
- $(M, *)$ je s krácením a s (jednoznačným) dělením.

Definice 1. 11. Nechť $M \neq \emptyset$. Je-li „$*$“ operace v M, pak struktura $(M, *)$ se nazývá grupoid.

Poznámka:
Je-li $(M, *)$ grupoid a na množině M definujeme operaci „$\circ$“ předpisem $a \circ b = b * a$ pro všechna $a, b \in M$, získáme grupoid $(M, \circ)$, který se nazývá opačný grupoid ke grupoidu $(M, *)$ a značí se $(M^{op}, *)$. Tyto grupoidy jsou totožné, právě když grupoid $(M, *)$ je komutativní.

Definice 1. 12. Struktura $(M, *)$ se nazývá asociativní grupoid neboli pologrupa, právě když $(M, *)$ je asociativní struktura. Je-li navíc komutativní nebo s neutrálním prvkem či s krácením atd., hovoříme o komutativní pologrupě nebo o pologrupě s neutrálním prvkem či s krácením atd. Pologrupa s neutrálním prvkem se nazývá monoid.

Lemma 1. 6. Nechť $(M, *)$ je komutativní pologrupa. Pak libovolné výrazy v $(M, *)$, které se liší pouze uzávorkováním nebo pořadím činitelů, jsou si rovny.

Poznámka:
Díky lemmatu 1. 6. můžeme v komutativní pologrupě psát:
$\{[(a * b) * (c * b)] * (a * c)\} * [(b * b) * (c * a)] = a * a * a * b * b * b * c * c * c.$

§ **1**

- Je-li $(M, *)$ pologrupa, $a \in M$ libovolný prvek, $n \in \mathbb{Z}^+$, pak definujeme prvek $a^{*n} \in M$ formulí:
  $a^{*n} = a * a * \ldots * a$ (n-krát) a nazýváme jej zobecněná mocnina.
  V případě multiplikativního a aditivního zápisu máme:
  $a^n = a \cdot a \cdot \ldots \cdot a$, jedná se o mocninu,
  $n \times a = a + a + \ldots + a$, mluvíme o přirozeném násobku.

- Ze způsobu zavedení zobecněné mocniny plynou tyto vztahy:
  $(\forall\, a \in M)\ \ a^{*1} = a,$
  $(\forall\, a \in M)\ (\forall\, n \in \mathbb{Z}^+)\ \ a^{*(n+1)} = a^{*n} * a.$
  V případě multiplikativního a aditivního zápisu dostáváme:
  $a^1 = a,\ a^{n+1} = a^n \cdot a;$
  $1 \times a = a,\ (n + 1) \times a = (n \times a) + a.$

- Je-li $m, n \in \mathbb{Z}^+$, pak zřejmě $(\forall\, a \in M)\ \ a^{*m} * a^{*n} = a^{*(m+n)} = a^{*n} * a^{*m}.$
  V případě multiplikativního a aditivního zápisu píšeme:
  $a^m a^n = a^{m+n} = a^n a^m,$
  $(m \times a) + (n \times a) = (m + n) \times a = (n \times a) + (m \times a).$

- Je-li $(M, *)$ monoid s neutrálním prvkem e, pak definujeme a^{*0} tak, že
  $a^{*0} = e, \forall\, a \in M.$
  Je-li $(M, \cdot)$ monoid s jednotkovým prvkem, pak $a^0 = 1$; pro monoid $(M, +)$ s nulovým prvkem píšeme $0 \times a = 0$.

Definice 1. 13. Grupoid, který je současně s krácením i s dělením, se nazývá kvazigrupa. Kvazigrupa s neutrálním prvkem se nazývá lupa.

Definice 1. 14. Struktura $(M, *)$ se nazývá grupa, právě když je asociativní, s neutrálním prvkem a s inverzními prvky. Je-li $(M, *)$ navíc komutativní, nazývá se komutativní (nebo též Abelova, abelovská) grupa.

Poznámka:

1) Tedy grupa je monoid, jehož každý prvek je invertibilní.
2) Někdy se grupa definuje jako asociativní kvazigrupa (tj. pologrupa s krácením a s dělením).
3) Jestliže $(M, *)$ je grupa, potom i opačný grupoid $(M^{op}, *)$ je grupa.

Příklad:

- $(\mathbb{N}, +)$…komutativní monoid s krácením, $(\mathbb{Z}, +)$…abelovská grupa
- $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$…komutativní monoid
- Nechť $M = \mathbb{Q}, \mathbb{R}, \mathbb{K}$
  $(M, +)$…abelovská grupa
  $(M, \cdot)$…komutativní monoid
  $(M - \{0\}, \cdot)$…abelovská grupa ($M - \{0\}$ se také značí M^*)

- Uvažujme množinu zbytkových tříd modulo m, tj. množinu:
  $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-2}, \overline{m-1}\}$, kde
  $\overline{i} = \{x \in \mathbb{Z};\ x = mk + i,\ 0 \leq i < m,\ k \in \mathbb{Z},\ m \in \mathbb{Z},\ m > 1\}$.
  V množině $\mathbb{Z}_m$ lze definovat operace „$\oplus$“, „$\odot$“:

  1) Předpisem, a to dvěma různými způsoby:
     a) $(\forall\ \overline{x}, \overline{y} \in \mathbb{Z}_m)$ $\overline{x} \oplus \overline{y} = \overline{z}$; je-li $x + y < m$, pak $z = x + y$
        je-li $x + y \geq m$, pak $z = x + y - m$
        $\overline{x} \odot \overline{y} = \overline{z}$; je-li $xy < m$, pak $z = xy$
        je-li $xy \geq m$, pak $z = xy - mq$, $q \in \mathbb{Z}$

     b) $(\forall\ \overline{x}, \overline{y} \in \mathbb{Z}_m)$ $\overline{x} \oplus \overline{y} = \overline{x + y}$; $\overline{x} \odot \overline{y} = \overline{xy}$.
        Dá se dokázat, že takto zavedené operace nezávisí na volbě reprezentantů (viz příklad 1. 1. 13 a)).

     Poznámka:
     Operace sčítání a násobení v $\mathbb{Z}$ jsou asociativní a komutativní, proto také operace „$\oplus$“, „$\odot$“ v $\mathbb{Z}_m$ jsou asociativní a komutativní (viz příklad 1. 1. 13 b)).

  2) Tabulkou:
     Uvažujme např. množinu $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

  - $(\mathbb{Z}_6, \oplus)$…abelovská grupa (s neutrálním prvkem $\overline{0}$)
  - $(\mathbb{Z}_6, \odot)$…komutativní monoid (s neutrálním prvkem $\overline{1}$)
  - $(\forall\ m \in \mathbb{Z})\ m > 1$ je $(\mathbb{Z}_m, \oplus)$ abelovská grupa a $(\mathbb{Z}_m, \odot)$ komutativní monoid.

Poznámka:
$(\mathbb{Z}_6 - \{\overline{0}\}, \odot) = (\mathbb{Z}_6^*, \odot)$…není algebraická struktura
$(\mathbb{Z}_p^*, \odot)$, kde p je prvočíslo…abelovská grupa

Definice 1. 15. Nechť $(G, *)$, $(H, \circ)$ jsou struktury. Pak $(H, \circ)$ se nazývá podstruktura struktury $(G, *)$, právě když platí:

1) $H \subseteq G$,
2) operace „$\circ$“ je restrikcí operace „$*$“ na množinu H (tj. $(\forall x, y \in H)\ x \circ y = x * y$).

Poznámka:

1) Restrikci i původní operaci můžeme značit stejným symbolem.
2) Jestliže nějaká vlastnost struktury platí i pro její podstrukturu, pak říkáme, že je to dědičná vlastnost (např. komutativnost, asociativnost).
3) Jestliže $(G, *)$ či $(H, \circ)$ je grupa nebo pologrupa, hovoříme o podgrupě grupy či pologrupy nebo o podpologrupě grupy či pologrupy.

Definice 1. 16. Nechť $(G, *)$, $(H, \circ)$ jsou struktury. Zobrazení F množiny G do množiny H se nazývá homomorfní zobrazení (homomorfismus), právě když platí:

$$(\forall x, y \in G)\ F(x * y) = F(x) \circ F(y) \quad \text{(tzv. podmínka homomorfismu).}$$

Je-li F homomorfismus struktury $(G, *)$ na strukturu $(H, \circ)$, pak se struktura $(H, \circ)$ nazývá homomorfní obraz struktury $(G, *)$.
Je-li F navíc bijekce, pak říkáme, že F je izomorfní zobrazení (izomorfismus) a struktura $(H, \circ)$ se nazývá izomorfní obraz struktury $(G, *)$.

Poznámka:

1) Složením dvou homomorfismů je opět homomorfismus.
2) Je-li F izomorfismus struktury $(G, *)$ na strukturu $(H, \circ)$, pak F^{-1} je izomorfismus $(H, \circ)$ na $(G, *)$. Říkáme, že struktury $(G, *)$, $(H, \circ)$ jsou navzájem izomorfní a píšeme $(G, *) \cong (H, \circ)$.

Definice 1. 17. Nechť $(G, *)$, $(H, \circ)$ jsou struktury. Řekneme, že strukturu $(H, \circ)$ lze izomorfně vnořit do struktury $(G, *)$, právě když existuje podstruktura $(G', *)$ struktury $(G, *)$ tak, že $(H, \circ) \cong (G', *)$.
Píšeme: $(H, \circ) \lhd (G, *)$.

Věta 1. 7. Nechť $(H, \circ)$ je homomorfní obraz struktury $(G, *)$ při homomorfismu F. Pak platí:

1) Je-li $(G, *)$ asociativní struktura, je i $(H, \circ)$ asociativní struktura.
2) Je-li $(G, *)$ komutativní struktura, je i $(H, \circ)$ komutativní struktura.
3) Je-li $(G, *)$ struktura s neutrálním prvkem e_G, je i $(H, \circ)$ struktura s neutrálním prvkem e_H a platí rovnost $e_H = F(e_G)$.
4) Jsou-li $(G, *)$, $(H, \circ)$ struktury s neutrálním prvkem a jsou-li prvky p, $\overline{p}$ navzájem inverzní v $(G, *)$, pak prvky $F(p)$, $F(\overline{p})$ jsou inverzními prvky v $(H, \circ)$ a platí: $\overline{F(p)} = F(\overline{p})$.

Důkaz:

1) Nechť $x, y, z \in H$ libovolné. Pak existují prvky $x_1, y_1, z_1 \in G$ takové, že $F(x_1) = x$, $F(y_1) = y$, $F(z_1) = z$. Tedy $(x \circ y) \circ z = (F(x_1) \circ F(y_1)) \circ F(z_1) = F(x_1 * y_1) \circ F(z_1) = F((x_1 * y_1) * z_1) = F(x_1 * (y_1 * z_1)) = F(x_1) \circ F(y_1 * z_1) = F(x_1) \circ (F(y_1) \circ F(z_1)) = x \circ (y \circ z)$.

2) Nechť $x, y \in H$ libovolné. Potom existují prvky $x_1, y_1 \in G$ tak, že $F(x_1) = x$, $F(y_1) = y$. Tedy $x \circ y = F(x_1) \circ F(y_1) = F(x_1 * y_1) = F(y_1 * x_1) = F(y_1) \circ F(x_1) = y \circ x$.

3) Nechť $e_G \in G$ je neutrální prvek struktury $(G, *)$. Pak existuje $F(e_G) = e_H \in H$. Musíme dokázat, že e_H je neutrální prvek struktury $(H, \circ)$. Je-li $x \in H$ libovolné, existuje $x_1 \in G$ tak, že $F(x_1) = x$. Potom $x \circ e_H = F(x_1) \circ F(e_G) = F(x_1 * e_G) = F(x_1) = x$ a současně $e_H \circ x = F(e_G) \circ F(x_1) = F(e_G * x_1) = F(x_1) = x$.
Tedy $e_H = F(e_G)$ je neutrální prvek struktury $(H, \circ)$.

4) Nechť prvky $p, \overline{p} \in G$ jsou navzájem inverzní v $(G, *)$. Pak existují $F(p), F(\overline{p}) \in H$; $F(p) \circ F(\overline{p}) = F(p * \overline{p}) = F(e_G) = e_H$ a zároveň $F(\overline{p}) \circ F(p) = F(\overline{p} * p) = F(e_G) = e_H$. Tedy $\overline{F(p)} = F(\overline{p})$. □

Důsledek věty 1. 7. Nechť $(G, *)$ je (abelovská) grupa. Pak její homomorfní, resp. izomorfní obraz je také (abelovská) grupa.

Poznámka:

1) Navzájem izomorfní struktury se, z algebraického hlediska, liší pouze označením prvků, resp. operací. Proto říkáme, že jsou až na izomorfismus totožné.
2) Injektivní homomorfismus se nazývá monomorfismus, surjektivní homomorfismus se nazývá epimorfismus.
3) Homomorfismus struktury do sebe se nazývá endomorfismus, izomorfismus struktury na sebe se nazývá automorfismus.

Příklad:

Uvažujme zobrazení F definované předpisem:

1) $F: (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}, +)$
   $(\forall\, x \in \mathbb{R}^+)\ \ F(x) = \log x$
2) $F: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$
   $(\forall\, x \in \mathbb{Z})\ \ F(x) = 2x - 2$

   Ověříme, zda se jedná o homomorfismus, příp. izomorfismus:

   ad 1)
   - F je bijekce
   - $(\forall\, x, y \in \mathbb{R}^+)\ \ F(x \cdot y) = \log (x \cdot y) = \log x + \log y = F(x) + F(y)$

   Tedy F je izomorfismus, tj. $(\mathbb{R}^+, \cdot) \cong (\mathbb{R}, +)$.

   ad 2)
   - $(\forall\, x, y \in \mathbb{Z})\ \ F(x + y) = 2(x + y) - 2 = 2x + 2y - 2$
     $F(x) + F(y) = 2x - 2 + 2y - 2 = 2x + 2y - 4$

   Tedy $F(x + y) \neq F(x) + F(y)$, tj. F není homomorfismus.

2. 2. Základní vlastnosti grup

V dalším, pokud nebude řečeno jinak, budeme užívat multiplikativní zápis grup, tj. budeme uvažovat grupy $(G, \cdot)$ s jednotkovým prvkem 1, inverzní prvek k prvku x grupy G budeme značit x^{-1}.

Věta 2. 1. Nechť $(G, \cdot)$ je grupa. Pak platí:

1) $(G, \cdot)$ je struktura s krácením.
2) $(G, \cdot)$ je struktura s jednoznačným dělením.
3) $(\forall\, x \in G)\ (x^{-1})^{-1} = x$.
4) $(\forall\, x, y \in G)\ (xy)^{-1} = y^{-1}x^{-1}$.
5) Jsou-li $x, y \in G$ takové, že $xy = y$ nebo $yx = y$, je x jednotkový prvek v $(G, \cdot)$.

Důkaz:

1), 2) Plyne ihned z lemmat 1. 3., 1. 5.

3) Nechť $x \in G$ je libovolný prvek. Pak existuje prvek $x^{-1} \in G$ tak, že $xx^{-1} = x^{-1}x = 1$, tedy $x^{-1}x = xx^{-1} = 1$. To ovšem znamená, že $(x^{-1})^{-1} = x$.

4) Má-li být $y^{-1}x^{-1}$ inverzní prvek k prvku xy, součiny $(xy)(y^{-1}x^{-1})$, $(y^{-1}x^{-1})(xy)$ musí být rovny jednotkovému prvku 1 v $(G, \cdot)$. Odvodíme postupně $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = (x1)x^{-1} = xx^{-1} = 1$ a zároveň $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}(1y) = y^{-1}y = 1$. Tedy máme $(xy)^{-1} = y^{-1}x^{-1}$.

5) Předpokládejme, že $x, y \in G$ jsou libovolné prvky a platí např. $xy = y$. Pak $x = x1 = x(yy^{-1}) = (xy)y^{-1} = yy^{-1} = 1$, takže x je jednotkový prvek grupy G. □

Věta 2. 2. Nechť $(G, \cdot)$ je asociativní struktura. Pak $(G, \cdot)$ je grupa, právě když G je struktura s dělením, tj. když platí:

$$(\forall\, x, y \in G)\ (\exists\, z, z' \in G)\ \ xz = y \wedge z'x = y.$$

Důkaz:

„$\Rightarrow$“: Je-li $(G, \cdot)$ grupa, je dokonce strukturou s jednoznačným dělením (podle věty 2. 1. 2)).

„$\Leftarrow$“: Nechť $(G, \cdot)$ je asociativní struktura s dělením.

- Protože $G \neq \emptyset$, existuje $a \in G$ a z podmínky dělení plyne existence prvku $e \in G$ tak, že $ea = a$. Dokážeme, že e je jednotkovým prvkem v G. Nechť tedy $b \in G$ a nechť $y \in G$ tak, že $ay = b$. Pak $(ea)y = ay$, dále díky asociativnosti můžeme psát $e(ay) = ay$ a podle zavedení y dostáváme $eb = b$. Označme e' takový prvek z G, pro nějž $ae' = a$ (ve struktuře s dělením musí existovat); analogicky předchozímu ukážeme, že $be' = b$. Pak platí $ee' = e$ a současně $ee' = e'$ (neboť pro každé $b \in G$ je $be' = b$ a také $eb = b$), tudíž $e = e'$. Tedy $(G, \cdot)$ je struktura s jednotkovým prvkem.
- Nechť $x \in G$ je libovolný prvek. Pak existují prvky $y_1, y_2 \in G$ tak, že $xy_1 = e$ a $y_2x = e$ (tj. inverzní prvky k x). Odtud díky asociativnosti dostáváme $(y_2x)y_1 = ey_1 = y_1$ a také $y_2(xy_1) = y_2e = y_2$, proto $y_1 = y_2$.

Tedy $(G, \cdot)$ je grupa. □

Věta 2. 3. Jediným idempotentním prvkem grupy $(G, \cdot)$ je její jednotkový prvek 1.

Důkaz:

Plyne ihned z věty 2. 1. 5). □

Definice 2. 1. Struktura $(H, \circ)$ se nazývá podgrupa grupy $(G, \cdot)$, právě když platí:

1) $H \subseteq G$,
2) operace „$\circ$“ je restrikcí operace „$\cdot$“ na množinu H,
3) $(H, \circ)$ je grupa.

Poznámka:

1) Každá grupa $(G, \cdot)$ obsahuje dvě tzv. triviální či nevlastní podgrupy: $(G, \cdot)$; $(\{1\}, \cdot)$ – jednotková podgrupa.
2) Každá podgrupa H grupy G taková, že $H \neq G$, $H \neq \{1\}$, se nazývá netriviální či vlastní podgrupa grupy G.
3) Jednotkový prvek grupy $(G, \cdot)$ je zároveň jednotkovým prvkem všech jejích podgrup.

Příklad:

- Struktury $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ jsou podgrupami grupy $(\mathbb{K}, +)$.
- Struktura $(S, +)$, kde $S = \{x \in \mathbb{Z};\ x = 2k,\ k \in \mathbb{Z}\}$ je podgrupou grupy $(\mathbb{Z}, +)$.

Věta 2. 4. Nechť $(G, \cdot)$ je grupa, $H \subseteq G$. Pak $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$, právě když platí:

1) $H \neq \emptyset$,
2) $(\forall\, x, y \in H)\ \ xy^{-1} \in H$.

Důkaz:

„$\Rightarrow$“: Předpokládejme, že $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$. Pak $(H, \cdot)$ je grupa, a tedy $H \neq \emptyset$ $(1 \in H)$. Jsou-li x, y libovolné prvky z H, je také $y^{-1} \in H$, a tedy $xy^{-1} \in H$.

„$\Leftarrow$“: Předpokládejme, že $H \subseteq G$ a zároveň platí podmínky 1) a 2).

- Protože $H \neq \emptyset$, existuje $x \in H$ a podle 2) je $xx^{-1} = 1 \in H$.
- Je-li $x \in H$ libovolný prvek, pak opět podle 2) dostáváme $1x^{-1} = x^{-1} \in H$.
- Předpokládejme, že $(H, \cdot)$ není asociativní. Pak existují $x, y, z \in H$ tak, že $(xy)z \neq x(yz)$ a současně $H \subseteq G$, tedy existují $x, y, z \in G$ tak, že $(xy)z \neq x(yz)$. To je ovšem spor s tím, že $(G, \cdot)$ je grupa, tj. $(H, \cdot)$ je asociativní.
  Tedy $(H, \cdot)$ je asociativní struktura s jednotkovým prvkem a s inverzními prvky, takže grupa.
- Jsou-li $x, y \in H$ libovolné, pak $y^{-1} \in H$, a tedy také $x(y^{-1})^{-1} = xy \in H$, takže operace v $(H, \cdot)$ je restrikcí operace v $(G, \cdot)$.

Tedy $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$. □

Je-li $(G, \cdot)$ konečná struktura (tj. množina G je konečná) a její operace „$\cdot$“ je zadaná Cayleyho tabulkou, pak $(G, \cdot)$ je grupa, právě když

- v každém řádku a v každém sloupci tabulky se každý prvek množiny G vyskytuje právě jednou,
- $(G, \cdot)$ je asociativní.

Nechť $(G, \cdot)$ je konečná grupa. Zda je $(H, \cdot)$ podgrupou grupy G poznáme z Cayleyho tabulky tak, že ověříme, zda pole, ve kterých se protínají řádky a sloupce tabulky označené prvky z množiny H, tvoří tabulku grupy.

Poznámka:

Systém všech podgrup dané grupy tvoří s relací „$\subseteq$“ uspořádanou množinu, můžeme jej proto znázornit Hasseovým diagramem.

§ 2

Nechť $(G, \cdot)$ je grupa, $g \in G$ libovolný prvek, $n \in \mathbb{Z}$. Pak definujeme celistvou mocninu g^n:

- je-li $n \geqq 0$, pak g^n definujeme podle § 1,
- je-li $n < 0$, pak $-n \in \mathbb{Z}^+$ a klademe $g^n = (g^{-1})^{-n}$ ve smyslu § 1.
- $(\forall g \in G)\ (\forall m, n \in \mathbb{Z})\ \ g^m g^n = g^{m+n}$,
  $(g^m)^n = g^{mn}$,
  $(g^n)^{-1} = g^{-n} = (g^{-1})^n$.
- Je-li grupa $(G, \cdot)$ komutativní, pak platí:
  $(\forall g, h \in G)\ (\forall\, n \in \mathbb{Z})\ \ (gh)^n = g^n h^n$.

Definice 2. 2. Je-li $(G, \cdot)$ konečná grupa, nazývá se počet prvků množiny G řád grupy $(G, \cdot)$ a značí se symbolem $|G|$. Je-li množina G, a tedy i grupa $(G, \cdot)$, nekonečná, pak říkáme, že grupa $(G, \cdot)$ má nekonečný řád, resp. je nekonečného řádu.

Definice 2. 3. Nechť $(G, \cdot)$ je grupa a g její libovolný prvek. Existuje-li nejmenší kladné celé číslo n tak, že $g^n = 1$, pak říkáme, že n je řád prvku g, resp. že prvek g je řádu n v grupě $(G, \cdot)$. Píšeme: $n = o(g)$, resp. $n = |g|$.
Jestliže takové číslo n neexistuje, pak říkáme, že prvek g je nekonečného řádu.

Věta 2. 5. Nechť g je libovolný prvek grupy $(G, \cdot)$. Je-li $o(g) = n$, pak pro každé $k \in \mathbb{Z}$ je $g^k = 1$, právě když $n \mid k$.
Důkaz:
„$\Longrightarrow$“: Předpokládejme, že $o(g) = n$ a $g^k = 1$, kde $k \in \mathbb{Z}$ libovolné. Tedy $n \in \mathbb{Z}^+$ je nejmenší takové, že $g^n = 1$, a podle věty o dělení se zbytkem v $\mathbb{Z}$ existují čísla $q, r \in \mathbb{Z}$ tak, že $k = nq + r$, $0 \leq r < n$. Potom $g^k = g^{nq+r} = g^{nq} g^r = (g^n)^q g^r = 1^q g^r = g^r = 1$, tedy $r = 0$ (vzhledem k volbě čísla n). To znamená, že $k = nq$, neboli $n \mid k$.
„$\Longleftarrow$“: Předpokládejme, že $o(g) = n$ a $n \mid k$, $k \in \mathbb{Z}$ libovolné. Tedy $g^n = 1$ a $k = nq$, $q \in \mathbb{Z}$. Pak $g^k = g^{nq} = (g^n)^q = 1^q = 1$. □

Poznámka:
Pro aditivní grupu $(G, +)$: n je řád prvku g, právě když $n \times g = 0$.

Věta 2. 6. Nechť $(G, \cdot)$ je grupa a $S = \{H_i\}_{i \in I}$ libovolný (i nekonečný) neprázdný systém jejích podgrup. Pak průnik $\bigcap_{i \in I} H_i$ všech podgrup systému S je rovněž podgrupa grupy G.
Důkaz:
Nechť je dána grupa $(G, \cdot)$ a libovolný neprázdný systém jejích podgrup $S = \{H_i\}_{i \in I}$. Označme P průnik všech H_i ze systému S, tj. $P = \bigcap_{i \in I} H_i$, $P \subseteq G$. Ukážeme, že P je podgrupa grupy G tak, že ověříme z věty 2. 4. podmínky 1), 2).

1) $P \neq \emptyset$ (každá z podgrup H_i obsahuje jednotkový prvek 1 grupy G, tedy $1 \in P$).
2) Nechť $x, y \in P$ jsou libovolné prvky. Pak $x, y \in H_i$ pro všechna $i \in I$, a tedy $xy^{-1} \in H_i$ pro všechna $i \in I$. To však znamená, že $xy^{-1} \in P$.

Tedy $P = \bigcap_{i \in I} H_i$ je podgrupa grupy $(G, \cdot)$. □

Definice 2. 4. Nechť $(G, \cdot)$ je grupa, X libovolná podmnožina v G. Průnik všech podgrup grupy G, které obsahují množinu X, je podgrupa v G, která se nazývá podgrupa generovaná množinou X a značí se $[X]$, resp. $\langle X \rangle$. Množina X se nazývá systém generátorů grupy $[X]$ a její prvky generátory této grupy.
Grupa G se nazývá konečně generovaná, jestliže existuje konečná množina X, která generuje grupu G, tj. $[X] = G$.

Poznámka:

1) Teprve věta 2. 6. dává definici 2. 4. smysl, neboť pro libovolnou množinu $X \subseteq G$ je systém všech podgrup grupy G obsahujících X neprázdný (jistě do něho patří grupa G), a tedy, podle zmíněné věty, jejich průnik je skutečně podgrupa grupy G.
2) $[X]$ je nejmenší (ve smyslu množinové inkluze „$\subseteq$“) podgrupa grupy G, která obsahuje množinu X, tj. pro libovolnou podgrupu H grupy G platí:
   je-li $X \subseteq H$, pak $[X] \subseteq H$.
3) Grupa může mít různé systémy generátorů. Je-li $(G, \cdot)$ grupa, pak $[G] = [G - \{1\}] = G$.
4) Je-li $X = \{x_1, x_2, \ldots, x_n\}$, pak píšeme $[X] = [\{x_1, x_2, \ldots, x_n\}] = [x_1, x_2, \ldots, x_n]$.
5) Je-li $X = \emptyset$, pak $[\emptyset] = (\{1\}, \cdot)$; píšeme: $[\emptyset] = [\{1\}] = [1]$.

Následující věta dává „vnitřní“ popis podgrupy generované množinou X.

Věta 2. 7. Nechť X je neprázdná podmnožina grupy $(G, \cdot)$. Potom podgrupa $[X]$ je množina právě všech prvků $h \in G$ tvaru:

$$h = x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n},$$

kde $x_1, x_2, \ldots, x_n$ je nějaká konečná posloupnost prvků z X (číslo n se mění) a $k_1, k_2, \ldots, k_n$ jsou celá čísla.

Důkaz:

Předpokládejme, že $\emptyset \neq X \subseteq G$, $(G, \cdot)$ je grupa.

Nechť $H = \{h \in G;\ h = x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n},\ x_i \in X,\ k_i \in \mathbb{Z},\ i = 1, \ldots, n\}$.

1) Dokážeme, že H je podgrupa grupy G obsahující X, takže $[X] \subseteq H$.
   - $\emptyset \neq X \subseteq H \subseteq G$, tj. $\emptyset \neq H \subseteq G$.
   - Nechť $h, g \in H$ jsou libovolné prvky, tedy $h = x_1^{k_1} \ldots x_n^{k_n}$, $g = x_1^{r_1} \ldots x_s^{r_s}$; protože $g \in G$, existuje $g^{-1} \in G$, $g^{-1} = (x_1^{r_1} \ldots x_s^{r_s})^{-1} = x_s^{-r_s} \ldots x_1^{-r_1}$ (viz § 2, věta 2. 1. 4)). Pak $hg^{-1} = x_1^{k_1} \ldots x_n^{k_n} \cdot x_s^{-r_s} \ldots x_1^{-r_1} \in H$.

   Podle věty 2. 4. je H podgrupa grupy G; protože $X \subseteq H$, je $[X] \subseteq H$.
2) Nechť $h \in H$ je libovolný prvek, tj. $h = x_1^{k_1} \ldots x_n^{k_n}$, $x_i \in X$, $k_i \in \mathbb{Z}$, $i = 1, \ldots, n$; poněvadž $x_i \in X$, je $x_i \in [X]$, proto také $x_i^{k_i} \in [X]$, odtud $x_1^{k_1} \ldots x_n^{k_n} \in [X]$, což znamená, že $h \in [X]$, a tedy $H \subseteq [X]$.

Dokázali jsme rovnost $H = [X]$, což je tvrzení věty. □

Věta 2. 8. Nechť $(G_1, *_1)$, $(G_2, *_2)$ jsou grupy. Definujme na množině $G_1 \times G_2$ operaci „$*$“ předpisem:

$$(\forall (x_1, x_2), (y_1, y_2) \in G_1 \times G_2)\ \ (x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2).$$

Pak $(G_1 \times G_2, *)$ je grupa.

Důkaz:

- Uzavřenost:
  Nechť $x_1, y_1 \in G_1$, $x_2, y_2 \in G_2$ jsou libovolné prvky. Pak $x_1 *_1 y_1 \in G_1$, $x_2 *_2 y_2 \in G_2$, a proto $(x_1 *_1 y_1, x_2 *_2 y_2) \in G_1 \times G_2$ pro všechny $(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$.
- Asociativnost:
  Jsou-li $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in G_1 \times G_2$ libovolné, pak $[(x_1, x_2) * (y_1, y_2)] * (z_1, z_2) =$
  $= (x_1 *_1 y_1, x_2 *_2 y_2) * (z_1, z_2) = ((x_1 *_1 y_1) *_1 z_1, (x_2 *_2 y_2) *_2 z_2) =$
  $= (x_1 *_1 (y_1 *_1 z_1), x_2 *_2 (y_2 *_2 z_2)) = (x_1, x_2) * (y_1 *_1 z_1, y_2 *_2 z_2) =$
  $= (x_1, x_2) * [(y_1, y_2) * (z_1, z_2)]$.

- Neutrální prvek:
  Nechť e_1 je neutrální prvek G_1, e_2 neutrální prvek G_2, nechť $(x_1, x_2) \in G_1 \times G_2$ je libovolná dvojice. Pak $(x_1, x_2) * (e_1, e_2) = (x_1 *_1 e_1, x_2 *_2 e_2) = (x_1, x_2)$ a zároveň také $(e_1, e_2) * (x_1, x_2) = (e_1 *_1 x_1, e_2 *_2 x_2) = (x_1, x_2)$. To znamená, že (e_1, e_2) je neutrální prvek $G_1 \times G_2$.
- Inverzní prvky:
  Je-li $(x_1, x_2) \in G_1 \times G_2$ libovolná, pak $(x_1, x_2) * (\overline{x}_1, \overline{x}_2) = (x_1 *_1 \overline{x}_1, x_2 *_2 \overline{x}_2) = (e_1, e_2)$ a současně $(\overline{x}_1, \overline{x}_2) * (x_1, x_2) = (\overline{x}_1 *_1 x_1, \overline{x}_2 *_2 x_2) = (e_1, e_2)$, tj. $\overline{(x_1, x_2)} = (\overline{x}_1, \overline{x}_2)$.
  Tedy $(G_1 \times G_2, *)$ je grupa. □

Definice 2. 5. Grupa $(G_1, *_1) \times (G_2, *_2) = (G_1 \times G_2, *)$ se nazývá direktní součin grup G_1, G_2.

Poznámka:

1) Počet prvků grupy $G_1 \times G_2$ je roven součinu počtu prvků grup G_1, G_2.
2) Analogicky můžeme zavést direktní součin grup $G_1,\ldots, G_n$, tedy grupu $(G_1, *_1) \times\ldots\times (G_n, *_n) = (G_1 \times\ldots\times G_n, *)$:

$$(\forall (x_1,\ldots, x_n), (y_1,\ldots, y_n) \in G_1 \times\ldots\times G_n)\ (x_1,\ldots, x_n) * (y_1,\ldots, y_n) = (x_1 *_1 y_1,\ldots, x_n *_n y_n).$$

Příklad:
Je-li $m, n \in \mathbb{Z}^+$, pak $(\mathbb{Z}_m, \oplus) \times (\mathbb{Z}_n, \oplus) = (\mathbb{Z}_m \times \mathbb{Z}_n, \oplus)$.

2. 3. Cyklické grupy

Definice 3. 1. Grupa, která má jednoprvkový systém generátorů $\{a\}$ (tj. grupa generovaná jednoprvkovou množinou $\{a\}$), se nazývá cyklická grupa. Místo $[\{a\}]$ píšeme pouze $[a]$, prvek a se nazývá generátor grupy $[a]$.

Věta 3. 1. Nechť $(G, \cdot)$ je cyklická grupa generovaná prvkem a, tedy $G = [a]$.
Pak $G = \{a^k; k \in \mathbb{Z}\}$.
Důkaz: Jde o bezprostřední důsledek věty 2. 7. pro $X = \{a\}$.

Poznámka:

1) Pro každé $x, y \in G$ existuje $k, l \in \mathbb{Z}$ tak, že $x = a^k$, $y = a^l$.
   Potom $xy = a^k a^l = a^{k+l} = a^{l+k} = a^l a^k = yx$, a tedy každá cyklická grupa je abelovská.
2) Uvažujeme-li aditivní grupu $(G, +)$, pak $G = \{k \times a; k \in \mathbb{Z}\}$.

Věta 3. 2. Nechť $G = [a]$ je cyklická grupa generovaná prvkem a. Pak jsou pouze tyto dvě možnosti:

1) Pro všechna $r, s \in \mathbb{Z}$, $r \neq s$, je $a^r \neq a^s$ a grupa $G = [a]$ je nekonečná.
2) Existuje $m \in \mathbb{Z}^+$ tak, že pro $r, s \in \mathbb{Z}$ je $a^r = a^s$, právě když $m \mid (r - s)$, neboli $a^r = 1$, právě když $m \mid r$. Odtud $|G| = o(a) = m$, neboť $G = \{a, a^2, \ldots, a^{m-1}, a^m = 1\}$.

Důkaz:
Podle věty 3. 1.: $G = [a] = \{a^k; k \in \mathbb{Z}\}$.

1) Jestliže pro každou dvojici $r, s \in \mathbb{Z}$, $r \neq s$, je $a^r \neq a^s$, je zřejmě grupa $[a]$ nekonečná.
2) Nenastane-li 1), pak existují $k, l \in \mathbb{Z}$, $k < l$, tak, že $a^k = a^l$, tedy $a^{l-k} = a^{k-k} = a^0 = 1$, což znamená, že existuje $t \in \mathbb{Z}^+$ takové, že $a^t = 1$. Nechť $m \in \mathbb{Z}^+$ je nejmenší takové, že $a^m = 1$. Je-li $k \in \mathbb{Z}$ libovolné, pak podle věty o dělení se zbytkem v $\mathbb{Z}$ existují $q, r \in \mathbb{Z}$ tak, že $k = mq + r$, $0 \leq r < m$.
   Potom $a^k = a^{mq+r} = (a^m)^q a^r = a^r$, takže $[a] = \{a^k; k \in \mathbb{Z}\} = \{a, a^2, \ldots, a^{m-1}, a^m = 1\}$.
   Jestliže $k = mq + r$ a přitom $0 < r < m$, pak $1 \neq a^r = a^k$ (vzhledem k volbě čísla m).
   Tedy $a^k = 1$, právě když $r = 0$, neboli právě když $m \mid k$. Odtud pro $r, s \in \mathbb{Z}$ dostáváme $a^r = a^s$, právě když $a^{r-s} = 1$, právě když $m \mid (r - s)$. Tedy libovolné dva z prvků $a, a^2, \ldots, a^{m-1}, a^m = 1$ jsou různé a $|G| = o(a) = m$. □

Poznámka:

1) Nastane-li možnost 1), pak $G = [a]$ je tzv. nekonečná cyklická grupa a prvek a je prvek nekonečného řádu; $G = [a] = \{\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = 1, a^1, a^2, a^3, \ldots\}$.
2) Nastane-li možnost 2), pak $G = [a]$ je tzv. konečná cyklická grupa a má řád m stejně jako její generátor, tj. prvek a;
   $G = [a] = \{a^1, a^2, \ldots, a^{m-1}, a^m = 1\} = \{a^0 = 1, a^1, a^2, \ldots, a^{m-1}\}$.

Věta 3. 3. Každá nekonečná cyklická grupa je izomorfní s aditivní grupou celých čísel $(\mathbb{Z}, +)$, a tedy libovolné dvě nekonečné cyklické grupy jsou navzájem izomorfní.
Důkaz:
Nechť $G = [a] = \{\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots\}$. Definujme zobrazení:
$\varphi: (\mathbb{Z}, +) \longrightarrow (G, \cdot) = ([a], \cdot)$
$(\forall k \in \mathbb{Z})\ \varphi(k) = a^k$

- φ je bijekce (zobrazení množiny $\mathbb{Z}$ na množinu G, které je injektivní, neboť G je nekonečná, a tedy podle věty 3. 2. je pro různá $r, s \in \mathbb{Z}$ také $\varphi(r) \neq \varphi(s)$),

- $(\forall\, k, l \in \mathbb{Z})\ \ \varphi(k + l) = a^{k+l} = a^k \cdot a^l = \varphi(k) \cdot \varphi(l)$ – splněna podmínka homomorfismu.

Tedy φ je izomorfismus, tj. $(\mathbb{Z}, +) \cong (G, \cdot)$. □

Poznámka:

1) Až na izomorfismus existuje jediná nekonečná cyklická grupa.
2) Je-li $k \in \mathbb{Z}$, pak množinu všech celistvých násobků čísla k, tj. množinu $\{kq;\ q \in \mathbb{Z}\}$, budeme značit symbolem $k\mathbb{Z}$. Zřejmě $(k\mathbb{Z}, +)$ je abelovská grupa, podgrupa grupy $(\mathbb{Z}, +)$.

Věta 3. 4. Grupa $(\mathbb{Z}, +)$ má pouze dva generátory, a to prvky 1 a –1.
Důkaz:

- Je-li $k \in \mathbb{Z}$, pak $[k] = k\mathbb{Z}$. Speciálně $[1] = \mathbb{Z} = [-1]$.
- Je-li $k \neq \pm 1$, pak $1 \notin k\mathbb{Z} = [k]$, a tedy $[k] \neq \mathbb{Z}$. □

Věta 3. 5. Nechť m je libovolné kladné celé číslo. Pak každá cyklická grupa řádu m je izomorfní s grupou $(\mathbb{Z}_m, \oplus)$, a tedy každé dvě cyklické grupy téhož (konečného) řádu jsou navzájem izomorfní.
Důkaz:
Nechť $G = [a] = \{a^0, a^1, \ldots, a^{m-1}\}$. Definujme zobrazení:
$\varphi: (\mathbb{Z}_m, \oplus) \longrightarrow (G, \cdot) = ([a], \cdot)$
$(\forall\, \overline{k} \in \mathbb{Z}_m)\ \ \varphi(\overline{k}) = a^k$

- φ je bijekce (injektivní zobrazení množiny $\mathbb{Z}_m$ na množinu G),
- $(\forall\, \overline{k}, \overline{l} \in \mathbb{Z}_m)\ \ \varphi(\overline{k} \oplus \overline{l}) = \varphi(\overline{k + l}) = a^{k+l} = a^k \cdot a^l = \varphi(\overline{k}) \cdot \varphi(\overline{l})$ – splněna podmínka homomorfismu.

Tedy φ je izomorfismus, tj. $(\mathbb{Z}_m, \oplus) \cong (G, \cdot)$. □

Poznámka:

1) Až na izomorfismus existuje jediná konečná cyklická grupa daného řádu.
2) Pro každé $m \in \mathbb{Z}$, $m > 1$: $(\mathbb{Z}_m, \oplus) = [\overline{1}]$ (neboť $m \times \overline{1} = \overline{0}$).

Definice 3. 2. Nechť $(G, \cdot)$ je grupa a a její libovolný prvek. Řádem prvku a v grupě G rozumíme řád cyklické podgrupy $[a]$ generované prvkem a.

Řády prvků tvoří důležitý invariant v důkazech, že dané dvě grupy nejsou izomorfní.

Věta 3. 6. Nechť $\varphi: G \longrightarrow H$ je izomorfismus grup. Pak $o(a) = o(\varphi(a))$ pro každé $a \in G$.
Důkaz:
Označme $n = o(a)$. Protože $\varphi^n(a) = \varphi(a^n)$ a φ je bijekce, platí $a^n = 1_G$ právě tehdy, když $\varphi(a^n) = \varphi(1_G)$, tj. když $\varphi^n(a) = 1_H$. □

Tedy pokud $G \cong H$, pak mají stejný počet prvků každého řádu. Opačná implikace neplatí. Např. grupy $G = \mathbb{Z}_2 \times \mathbb{Z}_8$ a $H = [a, x;\ a^2 = x^8 = 1,\ ax = x^5a]$ (viz příklad 8. 4) jsou řádu 16, obě mají jeden prvek řádu 1 (neutrální prvek), tři prvky řádu 2, čtyři prvky řádu 4 a osm prvků řádu 8, ale nejsou izomorfní (G je abelovská grupa, avšak H nikoli).

Příklad:
Jestliže $m, n \in \mathbb{Z}^+$, $nsd(m, n) > 1$, pak grupy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ nejsou izomorfní, protože grupa $\mathbb{Z}_{mn}$ obsahuje prvek $\overline{1}$ řádu mn, ale grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ má všechny prvky řádu nejvýše $nsn(m, n)$ (pro $nsd(m, n) > 1$ je totiž $nsn(m, n) < mn$).

Poznámka k příkladu:
Jestliže $nsd(m, n) = 1$, pak $(\mathbb{Z}_{mn}, \oplus) \cong (\mathbb{Z}_m, \oplus) \times (\mathbb{Z}_n, \oplus)$, a to na základě tvrzení:

Nechť $m_1, \ldots, m_n$ jsou po dvou nesoudělná kladná celá čísla, označme $M = m_1 \ldots m_n$. Pak $(\mathbb{Z}_M, \oplus) \cong (\mathbb{Z}_{m_1}, \oplus) \times \ldots \times (\mathbb{Z}_{m_n}, \oplus)$. – Čínská věta o zbytcích

Lemma 3. 7. Nechť a, b jsou prvky konečných řádů v grupě G takové, že $ab = ba$, tedy prvky a, b komutují. Jestliže $o(a) = m$, $o(b) = n$ a $nsd(m, n) = 1$, potom $o(ab) = |[ab]| = mn$.
Důkaz: Viz [7].

Věta 3. 8. Nechť $a_1, a_2, \ldots, a_k$ jsou prvky konečných řádů v grupě G, $o(a_i) = n_i$ $(i = 1, 2, \ldots, k)$. Jestliže $a_i a_j = a_j a_i$ a $nsd(n_i, n_j) = 1$, kdykoliv $i \neq j$ $(1 \leq i, j \leq k)$, potom $g = a_1 a_2 \ldots a_k$ je rovněž konečného řádu, a to $o(g) = |[a_1 a_2 \ldots a_k]| = n_1 n_2 \ldots n_k$.
Důkaz: Viz [7].

Věta 3. 9. Každá podgrupa cyklické grupy je cyklická grupa. Přitom každá nejednotková podgrupa nekonečné cyklické grupy je nekonečná.
Důkaz:
Nechť H je podgrupa cyklické grupy $G = [a]$. Pro $H = \{1\}$ je $H = [1]$, a proto předpokládejme, že $H \neq \{1\}$. Pak existuje $1 \neq h \in H$, a také $1 \neq h^{-1} \in H$. Jelikož $h \in H \subseteq G = [a]$, lze psát $h = a^k$, $h^{-1} = a^{-k}$, kde $k \in \mathbb{Z} - \{0\}$; tedy aspoň jedno z čísel $k, -k$ je kladné celé.
Nechť $d \in \mathbb{Z}^+$ je nejmenší takové, že $a^d \in H$; dokážeme, že $H = [a^d]$.

- Nechť a^n $(n \in \mathbb{Z})$ je libovolný prvek z H a pišme $n = dq + r$, kde $q, r \in \mathbb{Z}$, $0 \leq r < d$. Pak $a^r = a^{n - dq} = a^n (a^d)^{-q} \in H$, a tudíž $r = 0$ (vzhledem k volbě čísla d). Potom ovšem $a^n = (a^d)^q \in [a^d]$, proto $H \subseteq [a^d]$.
- Zřejmě $[a^d] \subseteq H$, takže dostáváme $H = [a^d]$.

Je-li $G = [a]$ nekonečná grupa, pak podle věty 3. 2. neexistuje $t \in \mathbb{Z}^+$ tak, aby $a^{dt} = 1$, a tedy podle téže věty je $[a^d]$ nekonečná grupa. □

Věta 3. 10. Homomorfní obraz cyklické grupy je cyklická grupa.
Důkaz:
Nechť $\varphi: G = [a] \longrightarrow H$ je epimorfismus.
Je-li $y \in H$ libovolný prvek, pak existuje $x \in G$ tak, že $\varphi(x) = y$. Protože $x \in G = [a]$, je $x = a^k$, $k \in \mathbb{Z}$, a tedy $\varphi(x) = \varphi(a^k) = \varphi^k(a) = y$. To znamená, že $H = [\varphi(a)]$. □

Poznámka:
Rovnost $\varphi(a^k) = \varphi^k(a)$ pro každé $a \in G$ a každé $k \in \mathbb{Z}$ plyne z vlastností homomorfismu:

- Pro $k > 0$ je $\varphi(a^k) = \varphi(aa \ldots a) = \varphi(a)\varphi(a) \ldots \varphi(a) = \varphi^k(a)$.
- Pro $k = 0$ je $\varphi(a^0) = \varphi(1_G) = 1_H = \varphi^0(a)$.
- Pro $k < 0$ je $\varphi(a^k) = \varphi((a^{-1})^{-k}) = \varphi^{-k}(a^{-1}) = (\varphi^{-k})^{-1}(a) = \varphi^k(a)$.

Věta 3. 11. Je-li $G = [a]$ konečná cyklická grupa řádu m, pak pro libovolné $k \in \mathbb{Z}$ je $G = [a^k]$, právě když $nsd(k, m) = 1$.
Důkaz:
Nechť $G = [a]$ je řádu m. Dokážeme, že $G = [a] = [a^k]$, právě když $nsd(k, m) = 1$.
„⇐“: Nechť $nsd(k, m) = 1$, pak existují $u, v \in \mathbb{Z}$ tak, že $ku + mv = 1$. Tedy $a = a^{ku + mv} = (a^k)^u (a^m)^v$ a zároveň $a^m = 1$ (podle věty 3. 2.), tedy $a = (a^k)^u \in [a^k]$, proto $[a] \subseteq [a^k]$. Obrácená inkluze, tj. $[a^k] \subseteq [a]$, je zřejmá: $(a^k)^u = a^{ku} = a^t$, $t \in \mathbb{Z}$.
Tedy $G = [a] = [a^k]$.

„$\Longrightarrow$“: Nechť $G = [a] = [a^k]$, $k \in \mathbb{Z}$. Pak $a \in [a] = [a^k]$, tedy $a = (a^k)^u$, odtud $1 = a^{ku-1}$, proto $m \mid ku - 1$ (podle věty 3. 2.). To znamená, že $ku - 1 = mv$, takže $ku - mv = 1$, neboli $ku + m(-v) = 1$. Tedy $nsd(k, m) = 1$. □

Věta 3. 12. Nechť $G = [a]$ je konečná cyklická grupa řádu m a nechť $d, n \in \mathbb{Z}^+$ tak, že $m = dn$. Pak $[a^d]$ je jediná podgrupa v G řádu n.

Důkaz:

Je-li $t \in \mathbb{Z}$, pak podle věty 3. 2. rovnost $(a^d)^t = 1$ nastává, právě když $m \mid dt$, neboli když $dn \mid dt$, a tedy právě když $n \mid t$. Pak ovšem podle téže věty číslo $n \in \mathbb{Z}^+$ udává počet prvků cyklické grupy $[a^d]$, takže $[a^d]$ je podgrupa v G řádu n. Nechť H je libovolná podgrupa v grupě $G = [a]$ řádu n. Z věty 3. 9. plyne, že $H = [a^k]$, $k \in \mathbb{Z}$, a z věty 3. 2. dostáváme jednak $(a^k)^n = a^{kn} = 1$, jednak $m \mid kn$. Tedy $kn = ml = ndl$, $l \in \mathbb{Z}$, neboli $k = dl$. Odtud $a^k = (a^d)^l$, takže $a^k \in [a^d]$. To však znamená, že $H = [a^k] \subseteq [a^d]$.

Podgrupy H a $[a^d]$ jsou obě řádu n, proto $H = [a^d]$. □

Věta 3. 13. Nechť $G = [a]$ je konečná cyklická grupa řádu m, $k \in \mathbb{Z}^+$, $d = nsd(k, m)$, $n \in \mathbb{Z}^+$ tak, že $m = dn$. Pak $H = [a^k]$ je podgrupa v G řádu n.

Důkaz:

Nechť $G = [a]$ je řádu m, $k \in \mathbb{Z}^+$, $d = nsd(k, m)$, $m = dn$, $n \in \mathbb{Z}^+$.
Dokážeme, že $H = [a^k]$ je podgrupa v G řádu n.

- Předpokládejme, že $d = nsd(k, m)$. To znamená, že $d \mid k$, neboli $k = dl$. Odtud dostáváme $a^k = (a^d)^l$, takže $H = [a^k] \subseteq [a^d]$.
- Existují $u, v \in \mathbb{Z}$ tak, že $d = ku + mv$; tedy $a^d = a^{ku+mv} = (a^k)^u(a^m)^v = (a^k)^u \in [a^k] = H$, čili $[a^d] \subseteq H$.

Tedy $H = [a^d]$ a zároveň $[a^d]$ je řádu n (podle věty 3. 12.), proto H je řádu n. □

Poznámka:

Nechť $G = [a]$ je konečná cyklická grupa řádu m. Definujme zobrazení $\varphi: \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ tak, že pro každé $m \in \mathbb{Z}^+$ je $\varphi(m)$ počet kladných celých čísel $k \leq m$ takových, že $nsd(k, m) = 1$. Zobrazení φ se nazývá Eulerova funkce.

1) Z věty 3. 2. plyne, že všechny prvky grupy G jsou vyčerpány posloupností navzájem různých mocnin $a, a^2, \ldots, a^{m-1}, a^m = 1$.

2) Z 1) a věty 3. 11. plyne, že $\varphi(m)$ udává počet všech různých generátorů grupy $G = [a]$. Je-li $m = p$, kde p je prvočíslo, pak grupa $G = [a]$ má právě $\varphi(p) = p - 1$ různých generátorů (všechny prvky kromě jednotkového prvku). Je-li $m = p^r$, kde p je prvočíslo a $r \in \mathbb{Z}^+$ libovolné číslo, pak grupa $G = [a]$ má právě $\varphi(p^r) = p^r - p^{r-1}$ různých generátorů (neboť mezi kladnými celými čísly $k \leq p^r$ jsou s p^r soudělná právě čísla $p, 2p, 3p, \ldots, p^{r-1} \cdot p$).
   Jestliže $n \in \mathbb{Z}^+$, $n \mid m$, pak vzhledem k větě 3. 12. existuje v G právě jedna podgrupa řádu n, a tedy G obsahuje právě $\varphi(n)$ prvků řádu n.

3) Z vět 3. 12. a 3. 13. plyne, že všechny podgrupy grupy $G = [a]$ jsou tvořeny množinou $\{[a^d]; d \in \mathbb{Z}^+, d \mid m\}$, resp. pro aditivní grupu množinou $\{[d \times a]; d \in \mathbb{Z}^+, d \mid m\}$.
   Je-li $m = p^r$ jako v 2), pak množina všech podgrup grupy G tvoří řetězec $r + 1$ do sebe vložených podgrup postupně řádů $1 = p^0, p^1, p^2, \ldots, p^r = m$.

2. 4. Rozklady podle podgrupy

Definice 4. 1. Nechť $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$, nechť $x \in G$. Množina $xH = \{xh; h \in H\}$ (resp. $Hx = \{hx; h \in H\}$) se nazývá levá (resp. pravá) třída grupy G podle podgrupy H určená prvkem x.

Věta 4. 1. Systém $S = \{xH\}_{x \in G}$ všech levých (resp. systém $S' = \{Hx\}_{x \in G}$ všech pravých) tříd grupy $(G, \cdot)$ podle podgrupy $(H, \cdot)$ představuje rozklad množiny G.
Důkaz:
Uvažujme $S = \{xH\}_{x \in G}$. Pak platí:

- $xH = \{xh; h \in H\} \subseteq G$, H je podgrupa G, tedy $H \neq \emptyset$, a proto také $xH \neq \emptyset$.
- Je-li $z \in G$ libovolné, lze psát $z = z1$, $1 \in H$, tedy $z \in zH$, odkud plyne $z \in \bigcup_{x \in G} xH$, tedy $G \subseteq \bigcup_{x \in G} xH$.
- Nechť $x, y \in G$ tak, že $xH \cap yH \neq \emptyset$. Pak existuje $z \in G$ takové, že $z \in xH$ a současně $z \in yH$, což znamená, že existují prvky $h_1, h_2 \in H$ tak, že $z = xh_1$ a také $z = yh_2$. Odtud $xh_1 = yh_2$, a tedy $x = yh_2h_1^{-1} = yh_3$, $y = xh_1h_2^{-1} = xh_4$, $h_3, h_4 \in H$. Nechť $u \in xH$ libovolné. Potom existuje $h \in H$ tak, že $u = xh = yh_3h$. Protože $h_3h \in H$, je $u \in yH$, takže $xH \subseteq yH$. Analogicky nechť $v \in yH$ libovolné. Potom existuje $h' \in H$ takové, že $v = yh' = xh_4h'$. Protože $h_4h' \in H$, je $v \in xH$, takže $yH \subseteq xH$. Tedy $xH = yH$.

Důkaz tvrzení o pravých třídách je obdobný nebo vyplyne z dokázaného přechodem k opačné grupě G^{op}. □

Poznámka:
Systém S (resp. S') z věty 4. 1. se nazývá rozklad grupy G na levé (resp. pravé) třídy podle podgrupy H.

Věta 4. 2. Nechť $(G, \cdot)$ je grupa, $(H, \cdot)$ její podgrupa. Pak pro každé $x \in G$ existuje bijekce množiny H na množinu xH (resp. na množinu Hx).
Důkaz:
Zobrazení $f: H \longrightarrow xH$ nechť je dáno předpisem $f(h) = xh$ (pro pevně zvolené $x \in G$). Zřejmě f je surjekce, neboť je-li $y \in xH$ libovolné, pak $y = xh_0$ pro některé $h_0 \in H$, tedy $f(h_0) = xh_0 = y$. Jestliže $f(h_1) = f(h_2)$, pak $xh_1 = xh_2$, odtud $h_1 = h_2$ (neboť grupa je struktura s krácením). Tedy f je injekce. Dohromady f je bijekce.

Pro množinu Hx analogicky. □

Poznámka:

1) Je-li H konečná množina, pak podle věty 4. 2. má každá množina xH (resp. Hx) stejný počet prvků jako množina H.
2) Z věty 4. 2. plyne, že lze na sebe bijektivně zobrazit i libovolné dvě levé (resp. pravé) třídy rozkladu S (resp. S'). Když například $f: H \leftrightarrow x_1H$, $g: H \leftrightarrow x_2H$, $f^{-1}: x_1H \leftrightarrow H$, pak $f^{-1} \circ g: x_1H \leftrightarrow x_2H$.

Věta 4. 3. Nechť $(G, \cdot)$ je grupa, $(H, \cdot)$ její podgrupa. Pak pro libovolné prvky $x, y \in G$ platí:

1) $xH = yH$, právě když $y^{-1}x \in H$, právě když $x^{-1}y \in H$.
2) $Hx = Hy$, právě když $yx^{-1} \in H$, právě když $xy^{-1} \in H$.

Důkaz:

1) - Z předpokladu $xH = yH$ plyne existence $h_1, h_2 \in H$ takových, že $xh_1 = yh_2$. Odtud dostáváme $y^{-1}xh_1 = h_2$, tedy $y^{-1}x = h_2h_1^{-1} = h \in H$. Takže $y^{-1}x \in H$.

Protože $y^{-1}x \in H$ a H je podgrupa, je také $(y^{-1}x)^{-1} = x^{-1}y \in H$.

- Z předpokladu $y^{-1}x \in H$ plyne existence $h \in H$ tak, že $y^{-1}x = h$, tedy $x = yh \in yH$. Protože $x = x1$, $1 \in H$, je také $x \in xH$. Tedy $xH \cap yH \neq \emptyset$, proto $xH = yH$.

2) Analogicky. □

Poznámka:
Uvažujeme-li aditivní grupu $(G, +)$, pak např. 2) věty 4. 3. má tvar:
$H + x = H + y$, právě když $y - x \in H$, právě když $x - y \in H$.

Věta 4. 4. Nechť S (resp. S') je rozklad grupy $(G, \cdot)$ na levé (resp. pravé) třídy podle její podgrupy $(H, \cdot)$. Pak existuje bijekce množiny S na množinu S'.
Důkaz:
Definujme zobrazení $f: S \longrightarrow S'$ takto: $(\forall\ xH \in S)\ \ f(xH) = Hx^{-1}$. Pak pro $xH, yH \in S$ libovolné platí rovnost $xH = yH$, právě když $y^{-1}x \in H$ (viz věta 4. 3.), neboli právě když $y^{-1}(x^{-1})^{-1} \in H$, a tedy podle téže věty 4. 3. právě když $Hx^{-1} = Hy^{-1}$ (tj. $f(xH) = f(yH)$). To znamená, že f je korektně definované zobrazení, které je zároveň injektivní. Protože f je zřejmě surjekce, jedná se o bijekci. □

Poznámka:
Podle věty 4. 4. mají tedy rozklady S a S' (při dané grupě G a podgrupě H) stejný počet prvků (v případě konečných množin S a S').

Definice 4. 2. Nechť $(G, \cdot)$ je grupa, $(H, \cdot)$ její podgrupa a S (resp. S') rozklad grupy G na levé (resp. pravé) třídy podle podgrupy H. Je-li S (resp. S') konečná množina, nazývá se počet jejích prvků (tj. počet levých (resp. pravých) tříd podle podgrupy H) index podgrupy H v grupě G a píšeme $[G : H]$. Je-li S (resp. S') nekonečná množina, říkáme, že podgrupa H má nekonečný index, resp. že je nekonečného indexu v G.

Poznámka:
Pokud chceme zdůraznit, že rozklad grupy G podle její podgrupy H je konečná množina, říkáme, že podgrupa H má konečný index, resp. že je konečného indexu v grupě G.

Věta 4. 5. (**Lagrangeova**) Nechť $(H, \cdot)$ je podgrupa konečné grupy $(G, \cdot)$. Pak platí:

$$|G| = |H| \cdot [G : H].$$

Důkaz:
Utvoříme rozklad S (resp. S') grupy G na levé (resp. pravé) třídy podle podgrupy H. Potom S (resp. S') má $[G : H]$ prvků (jimiž jsou po dvou disjunktní levé (resp. pravé) třídy, jejichž sjednocením je množina G). Podle věty 4. 2. mají všechny levé (resp. pravé) třídy stejný počet prvků, a to $|H|$, tedy počet prvků grupy G, tj. $|G|$ je roven $|H| \cdot [G : H]$. □

Důsledky věty 4. 5.

1) Nechť $(G, \cdot)$ je konečná grupa a $(H, \cdot)$ její podgrupa. Pak řád podgrupy H dělí řád grupy G, tj. $|H|$ dělí $|G|$.

2) Je-li G konečná grupa, pak řád každého prvku grupy G dělí $|G|$.
Důkaz:
Nechť $|G| = m$, $g \in G$ libovolné. Je-li $g = 1$, pak $o(g) = 1$, a tedy $1 \mid m$. Je-li $g \neq 1$, pak $[g]$ je podgrupa grupy G stejného řádu, jako je řád prvku g, a tedy $o(g) \mid m$. □

3) Každá grupa prvočíselného řádu je cyklická.
   Důkaz:
   Nechť G je grupa prvočíselného řádu p, tj. $|G| = p$. Je-li $1 \neq g \in G$ libovolné, pak podle důsledku 1) řád podgrupy $[g]$ dělí p. Protože $1 < |[g]| = o(g)$, je $|[g]| = p$, takže $G = [g]$. □

Věta 4. 6. Jsou-li H, K podgrupy konečného indexu v grupě G, potom $H \cap K$ je rovněž podgrupa konečného indexu v G.
Důkaz:
Nejdříve ukážeme, že když $g \in G$, pak $g(H \cap K) = gH \cap gK$. Protože $g(H \cap K) \subseteq gH$ a také $g(H \cap K) \subseteq gK$, je $g(H \cap K) \subseteq gH \cap gK$. Je-li však $x \in gH \cap gK$, je $x = gh = gk$ pro vhodné prvky $h \in H$ a $k \in K$. Odtud $g^{-1}x = h = k \in H \cap K$, nebo-li $x = g(g^{-1}x) \in g(H \cap K)$, tedy platí i obrácená inkluze $gH \cap gK \subseteq g(H \cap K)$. Z rovnosti $g(H \cap K) = gH \cap gK$ plyne, že každá levá třída grupy G podle podgrupy $H \cap K$ (jde o podgrupu na základě věty 2. 6.) se získá jako průnik některé levé třídy podle H s některou levou třídou podle K. Je-li tedy $[G : H] = m$ a $[G : K] = n$, pak $[G : (H \cap K)] \leq mn$. □

Věta 4. 7. (**Poincarého**) Jsou-li $H_1, H_2, \ldots, H_n$ podgrupy konečného indexu v grupě G, potom $H = \bigcap_{i=1}^{n} H_i$ je rovněž podgrupa konečného indexu v G.
Důkaz:
Věta se dokáže úplnou indukcí podle čísla n pomocí věty 4. 6. □

Nechť H je podgrupa grupy G; neprázdná množina $A \subseteq G$ se nazývá úplný systém reprezentantů levých tříd grupy G podle podgrupy H, jestliže pro každé $g \in G$ existuje právě jeden prvek $a \in A$ takový, že $gH = aH$. V takovém případě $\{aH\}_{a \in A}$ je systém všech levých tříd grupy G podle podgrupy H a $|A| = [G : H]$. Přitom úplné systémy reprezentantů vždy existují.

Věta 4. 8. Nechť H, K jsou podgrupy grupy G takové, že $K \subseteq H$. Pak platí:

$$[G : K] = [G : H] \cdot [H : K].$$

Důkaz:
Nechť množina $A \subseteq G$ (resp. $B \subseteq H$) je úplný systém reprezentantů levých tříd grupy G podle podgrupy H (resp. grupy H podle podgrupy K). Je-li $g \in G$ libovolné, pak existuje $a \in A$ tak, že $gH = aH$, načež $a^{-1}g \in H$ (viz věta 4. 3.). Tedy pro vhodné $b \in B$ bude $a^{-1}gK = bK$, čili $gK = abK$. Uvažujme dále prvky $a_1, a_2 \in A$, $b_1, b_2 \in B$ tak, že $a_1b_1K = a_2b_2K$. Pro vhodné $k \in K$ je tedy $a_1b_1 = a_2b_2k$, takže (protože prvky b_1, b_2, k leží v H) $a_1H = a_1b_1H = a_2b_2kH = a_2H$, a proto $a_1 = a_2$. Pak ovšem z rovnosti $a_1b_1K = a_2b_2K$ plyne rovnost $b_1K = b_2K$ (v grupě lze krátit), a tudíž $b_1 = b_2$. Odtud jednak plyne, že množina AB je úplný systém reprezentantů levých tříd grupy G podle podgrupy K, zároveň ale, že každý prvek $x \in AB$ lze zapsat ve tvaru $x = ab$ ($a \in A$, $b \in B$) právě jedním způsobem. To ovšem znamená, že $[G : K] = |AB| = |A| \cdot |B| = [G : H] \cdot [H : K]$. □

Definice 4. 3. Nechť $(G, \cdot)$ je grupa. Řekneme, že podgrupa N grupy G je normální podgrupa v G, právě když platí:

$$(\forall\, g \in G)\ \ gN = Ng. \qquad \text{Píšeme: } N \trianglelefteq G.$$

Poznámka:
1) Rozklady grupy na levé a pravé třídy podle normální podgrupy se rovnají, tj. $S = S'$.
2) V komutativní (a tedy také v cyklické) grupě je zřejmě každá podgrupa normální.

3) Každá nekomutativní grupa má vždy alespoň dvě normální podgrupy, a to jednotkovou podgrupu $\{1\}$ a grupu G:
   - je-li $N = \{1\}$, pak $S = \{xN\}_{x\in G} = \{x\{1\}\}_{x\in G} = \{\{x\}\}_{x\in G} = \{\{1\}x\}_{x\in G} = \{Nx\}_{x\in G} = S'$;
   - je-li $N = G$, pak $S = \{xG\}_{x\in G} = \{G\} = \{Gx\}_{x\in G} = S'$.
4) Existují (nekomutativní) grupy, které nemají jiné normální podgrupy než $\{1\}$ a G.

Lemma 4. 9. Podgrupa N grupy G je normální podgrupou v G, právě když platí:

$$(\forall\, g \in G)\ (\forall\, n \in N)\ (\exists\, n_1, n_2 \in N)\ \ (gn = n_1 g \wedge ng = gn_2).$$

Důkaz:

„$\Longrightarrow$“: Předpokládejme, že $N \trianglelefteq G$. Pak pro každé $g \in G$ je $gN = Ng$, tedy $gN \subseteq Ng$ a zároveň $Ng \subseteq gN$. Tedy pro každé $n \in N$ je $gn \in Ng$ a zároveň $ng \in gN$, což znamená, že existují $n_1, n_2 \in N$ tak, že $gn = n_1 g$ a zároveň $ng = gn_2$.

„$\Longleftarrow$“: Analogicky. □

Věta 4. 10. Podgrupa N grupy G je normální podgrupou v G, právě když platí:
1) $(\forall\, g \in G)\ \ gNg^{-1} \subseteq N$ (resp. $g^{-1}Ng \subseteq N$),
2) $(\forall\, g \in G)\ (\forall\, n \in N)\ \ gng^{-1} \in N$ (resp. $g^{-1}ng \in N$).

Důkaz:

2) „$\Longrightarrow$“: Předpokládejme, že $N \trianglelefteq G$, $x = gng^{-1}$. Protože $N \trianglelefteq G$, lze psát $gn = n_1 g$ pro jisté $n_1 \in N$ (viz lemma 4. 9.). Tedy $x = gng^{-1} = (n_1 g)g^{-1} = n_1(gg^{-1}) = n_1 \in N$, takže $x \in N$.

   „$\Longleftarrow$“: Předpokládejme, že platí podmínka 2). Dokážeme, že pro libovolné $g \in G$ je $gN = Ng$.
   - Nechť $x \in gN$ libovolné. Pak existuje $n \in N$ tak, že $x = gn$. Tedy $xg^{-1} = gng^{-1}$ a zároveň $gng^{-1} \in N$, proto také $xg^{-1} \in N$. To znamená, že existuje $n_1 \in N$ tak, že $xg^{-1} = n_1$, odkud $xg^{-1}g = n_1 g$, takže $x = n_1 g$, což je prvek z Ng.
     Tedy $gN \subseteq Ng$.
   - Nechť $x \in Ng$ libovolné. Pak existuje $n \in N$ tak, že $x = ng$. Tedy $g^{-1}x = g^{-1}ng$ a zároveň $g^{-1}ng \in N$, proto $g^{-1}x \in N$, což ovšem znamená, že existuje $n_1 \in N$ takové, že $g^{-1}x = n_1$, takže $x = gn_1$, což je prvek z gN.

     Tedy $Ng \subseteq gN$. □

Věta 4. 11. Nechť H je podgrupa grupy G. Jestliže $[G : H] = 2$, pak $H \trianglelefteq G$.

Důkaz:

Je-li $[G : H] = 2$, pak v G existují právě dvě různé levé třídy, a to $H = 1H$, druhá je aH pro některé $a \notin H$. Nechť $h \in H$, $g \in G$. Předpokládejme, že $g^{-1}hg \notin H$.

- Jestliže $g \in H$, pak $g^{-1} \in H$, neboť H je podgrupa, a tedy $g^{-1}hg \in H$, což je spor.
- Jestliže $g \notin H$, pak $g^{-1} \notin H$, tedy $g^{-1}H \neq H$. Jelikož $[G : H] = 2$, je $aH = g^{-1}H$, a tedy $g^{-1}hg \notin H$, takže $g^{-1}hg \in g^{-1}H$. Odtud dostáváme $g^{-1}hg = g^{-1}h_0$ pro některé $h_0 \in H$, tedy $hg = h_0$, tj. $g = h^{-1}h_0 \in H$, což je opět spor. Musí tedy platit $g^{-1}hg \in H$, tj. $H \trianglelefteq G$ (podle věty 4. 10.). □

Věta 4. 12. Průnik libovolného neprázdného systému normálních podgrup grupy G je opět normální podgrupa grupy G.

Důkaz:

Nechť N_i $(i \in I \neq \emptyset)$ jsou normální podgrupy grupy G a položme $N = \bigcap_{i\in I} N_i$.

- Podle věty 2. 6. je N podgrupa v G.
- Je-li $g \in G$, $n \in N$ libovolné, pak $n \in N_i$ pro každé $i \in I$, a tedy také $gng^{-1} \in N_i$ pro každé $i \in I$ (neboť $N_i \trianglelefteq G$), takže $gng^{-1} \in N$. Odtud $N \trianglelefteq G$. □

Poznámka:
Je-li X podmnožina v G, pak průnik všech normálních podgrup grupy G, které obsahují množinu X, se nazývá normální podgrupa grupy G generovaná množinou X. Ve smyslu množinové inkluze „$\subseteq$“ je to nejmenší normální podgrupa grupy G obsahující množinu X.

Definice 4. 4. Nechť G je grupa a $x, y \in G$ libovolné prvky. Řekneme, že prvek y je v grupě G konjugován s prvkem x (resp. že prvky x, y jsou v grupě G konjugované), existuje-li $g \in G$ tak, že $y = g^{-1}xg$. Píšeme $x \sim y$.

Poznámka:
1) Relace „$\sim$“ je ekvivalence na množině G (tj. reflexivní, symetrická a tranzitivní):
   - $x = 1^{-1}x1$, tedy $x \sim x$ pro každé $x \in G$;
   - je-li $x \sim y$, pak existuje $g \in G$ tak, že $y = g^{-1}xg$, tedy $gy = xg$, odtud $gyg^{-1} = x$, což můžeme zapsat jako $(g^{-1})^{-1}yg^{-1} = x$; označme $g^{-1} = h \in G$, tedy $h^{-1}yh = x$, tj. $y \sim x$ pro každé $x, y \in G$;
   - je-li $x \sim y$ a zároveň $y \sim z$, pak existuje $g, h \in G$ tak, že $y = g^{-1}xg$ a zároveň $z = h^{-1}yh$, tedy $z = h^{-1}(g^{-1}xg)h = (h^{-1}g^{-1})x(gh) = (gh)^{-1}x(gh)$, $gh \in G$, tj. $x \sim z$ pro každé $x, y, z \in G$.

   Tedy relace „$\sim$“ indukuje na množině G rozklad na třídy spolu konjugovaných prvků.
2) Jsou-li g, x prvky grupy G, potom prvek $g^{-1}xg$ se často zapisuje symbolicky x^g; tedy $g^{-1}xg = x^g$. Množina všech prvků z G konjugovaných s prvkem x je tedy $\{x^g; g \in G\}$, neboli stručně $\{x^g; g \in G\} = x^G$.

Věta 4. 13. Podgrupa N grupy G je normální podgrupou v G, právě když s každým svým prvkem obsahuje i všechny prvky, které jsou s ním v G konjugované.
Důkaz:
„$\Rightarrow$“: Předpokládejme, že $N \trianglelefteq G$. Pak pro každé $g \in G$ a každé $n \in N$ je $g^{-1}ng \in N$, tedy existuje $n_1 \in N$ tak, že $n_1 = g^{-1}ng$, odtud $n \sim n_1$.
„$\Leftarrow$“: Nechť $n \in N$ libovolné, nechť $n_2 \in N$ takový, že $n \sim n_2$. Pak $n_2 = g^{-1}ng$, $g \in G$, takže $g^{-1}ng \in N$, tedy $N \trianglelefteq G$. □

Definice 4. 5. Řekneme, že podgrupa K je v grupě G konjugovaná s podgrupou H, právě když je $K = g^{-1}Hg$ pro nějaké $g \in G$. Píšeme $H \sim K$.

Poznámka:
1) Je-li G grupa a $\mathscr{L}(G)$ množina všech podgrup grupy G, pak relace „$\sim$“ konjugovanosti podgrup je ekvivalence na množině $\mathscr{L}(G)$.
2) Je-li $H \in \mathscr{L}(G)$ a $g \in G$, pak místo $g^{-1}Hg$ je možno opět psát H^g; potom třída všech podgrup grupy G konjugovaných s podgrupou H je systém $\{H^g; g \in G\}$, což můžeme symbolicky psát H^G.

Definice 4. 6. Je-li M neprázdná podmnožina grupy G, potom normalizátorem $N_G(M)$ množiny M v grupě G rozumíme množinu všech prvků $g \in G$ takových, že $g^{-1}Mg = M$ (neboli $gM = Mg$). Normalizátor jednoprvkové množiny $\{a\}$ značíme $N_G(a)$.

Věta 4. 13. Nechť G je grupa a $x \in G$ libovolný prvek. Pak platí:

1) $N_G(x)$ je podgrupa grupy G.
2) Je-li A množina všech prvků z grupy G konjugovaných s prvkem x, tedy $A = x^G$, pak $|A| = |x^G| = [G : N_G(x)]$.

Věta 4. 14. Je-li H podgrupa grupy G, pak $N_G(H)$ je největší (ve smyslu množinové inkluze „$\subseteq$“) podgrupa grupy G taková, že $H \trianglelefteq N_G(H)$.

Věta 4. 15. Nechť H je podgrupa grupy G a nechť $\mathscr{A}$ je množina všech podgrup konjugovaných v grupě G s podgrupou H. Pak platí:

1) $|\mathscr{A}| = [G : N_G(H)]$.
2) Průnik všech podgrup z $\mathscr{A}$ je normální podgrupou v G.

Věta 4. 16. Nechť G je grupa. Pak platí:

1) Jsou-li podgrupy H, K v grupě G konjugované, pak i jejich normalizátory $N_G(H)$, $N_G(K)$ jsou v G konjugované a platí rovnost $[G : H] = [G : K]$.
2) Jsou-li prvky $a, b \in G$ v grupě G konjugované, pak i jejich normalizátory $N_G(a)$, $N_G(b)$ jsou v G konjugované.

Věta 4. 17. Nechť H je podgrupa konečného indexu v grupě G. Pak v G existuje normální podgrupa N konečného indexu taková, že $N \subseteq H$.

Poznámka:
Důkazy vět 4. 13. – 4. 17. uvedeny v [7].

Definice 4. 7. Grupa G se nazývá jednoduchá, jestliže je netriviální (tj. $G \neq \{1\}$) a G, $\{1\}$ jsou jediné normální podgrupy grupy G.

Věta 4. 18. Grupa G je jednoduchá komutativní grupa, právě když G je cyklická grupa prvočíselného řádu.

Důkaz:

„$\Rightarrow$“: Předpokládejme, že G je jednoduchá komutativní grupa, tj. G má pouze dvě triviální podgrupy. Nechť $1 \neq g \in G$ je libovolný prvek. Pak g generuje podgrupu grupy G, která je různá od podgrupy $\{1\}$, tedy $[g] = G$. To znamená, že G je cyklická. Kdyby grupa $[g]$ byla nekonečná, pak z věty 3. 2. by plynulo $g \notin [g^2]$, což by znamenalo, že $[g^2]$ je vlastní podgrupa grupy G; tedy grupa $G = [g]$ je konečná řádu $m > 1$. Cyklická grupa řádu m má právě tolik podgrup, kolik kladných dělitelů má číslo m. Protože G má právě dvě podgrupy, číslo m má právě dva dělitele; tedy m je prvočíslo.

„$\Leftarrow$“: Předpokládejme, že G je cyklická grupa prvočíselného řádu.

- Každá cyklická grupa je komutativní, tj. G je komutativní grupa, která je netriviální (neboť je prvočíselného řádu).
- Každá podgrupa grupy G je cyklická (podle věty 3. 9.). Pro $1 \in G$ je $[1] = \{1\}$, je-li $1 \neq g \in G$ libovolný prvek, pak $[g] = G$. To znamená, že v G existují pouze dvě podgrupy, a to $\{1\}$ a G.

  Tedy G je jednoduchá komutativní grupa. □

Věta 4. 19. Nechť N je normální podgrupa grupy $(G, \cdot)$. Rozklad S (resp. S') grupy G na levé (resp. pravé) třídy podle podgrupy N tvoří grupu vzhledem k operaci „$\cdot$“ definované takto:

$$(\forall\, xN, yN \in S)\ \ (xN)(yN) = xyN \quad (\text{resp. } (\forall\, Nx, Ny \in S')\ \ (Nx)(Ny) = Nxy.$$

Důkaz:

Protože N je normální podgrupa grupy G, tj. pro každé $x \in G$ je $xN = Nx$, stačí tvrzení dokázat pouze pro rozklad např. na levé třídy.

Předpokládejme tedy, že $N \trianglelefteq G$, $S = \{xN\}_{x \in G}$.

- Nechť $xN, yN \in S$ libovolné. Pak $(xN)(yN) = x(Ny)N = x(yN)N = xy(NN) = xyN \in S$.
- Nechť $xN, yN, zN \in S$ libovolné. Pak $[(xN)(yN)](zN) = (xyN)(zN) = xyzN = x(yzN) = (xN)(yzN) = (xN)[(yN)(zN)]$.
- Nechť $xN \in S$ libovolné. Pak $(xN)N = (xN)(1N) = x1N = xN$ a také $N(xN) = (1N)(xN) = 1xN = xN$. Tedy $N = 1N$ je neutrální prvek v S.
- Je-li $x \in G$, pak existuje $x^{-1} \in G$. Nechť $xN \in S$ libovolné. Potom $(xN)(x^{-1}N) = xx^{-1}N = 1N = N$ a také $(x^{-1}N)(xN) = x^{-1}xN = 1N = N$. To znamená, že $(xN)^{-1} = x^{-1}N$.

Tedy $(S, \cdot)$ je grupa. □

Definice 4. 8. Nechť $(G, \cdot)$ je grupa, N normální podgrupa v G. Pak grupa $(S, \cdot)$ (resp. $(S', \cdot)$), kde operace „$\cdot$“ je definovaná předpisem z věty 4. 19., se nazývá faktorová grupa (nebo též faktorgrupa) grupy G podle normální podgrupy N a značí se $(G/N, \cdot)$.

Faktorovou grupu je možné zavést ještě jiným způsobem. Máme-li dánu nějakou grupu $(G, \cdot)$, může být rozklad množiny G zadán také jako rozklad podle jisté ekvivalence R definované na G. Tento rozklad se nazývá rozklad indukovaný ekvivalencí R a značí se G/R. Třídy tohoto rozkladu jsou podmnožiny $\square Rx$ množiny G definované takto: $(\forall\, x \in G)\ \ \square Rx = \{y \in G;\, yRx\}$. Je tedy $G/R = \{\square Rx\}_{x \in G}$.

Poznámka:

Místo tříd rozkladu $\square Rx$ množiny G můžeme uvažovat třídy $xR\square$ definované analogicky: $(\forall\, x \in G)\ \ xR\square = \{y \in G;\, xRy\}$. Díky symetričnosti ekvivalence totiž platí $xR\square = \square Rx$.

Definice 4. 9. Nechť $(G, \cdot)$ je grupa, R relace na množině G. Pak R se nazývá kongruence v grupě $(G, \cdot)$, právě když R je ekvivalence a platí:

$$(\forall\, x_1, x_2, y_1, y_2 \in G)\ \ x_1Rx_2 \wedge y_1Ry_2 \Longrightarrow x_1y_1Rx_2y_2.$$

Vybereme-li na G takovou relaci R, která je kongruencí, pak pro libovolné $\square Rx, \square Ry \in G/R$ je $\square Rx \cdot \square Ry = \square Rxy \in G/R$.

Věta 4. 20. Nechť $(G, \cdot)$ je grupa, R relace kongruence na G. Pak struktura $(G/R, \cdot)$ je také grupou.

Důkaz:

Předpokládejme, že $(G, \cdot)$ je grupa, R kongruence na G.

- Pro všechny $\square Rx, \square Ry \in G/R$ je $\square Rx \cdot \square Ry = \square Rxy \in G/R$, tedy G/R je uzavřená vzhledem k „$\cdot$“.

- Asociativnost $(G/R, \cdot)$:
  Nechť $\square Rx, \square Ry, \square Rz \in G/R$ libovolné. Pak $(\square Rx \cdot \square Ry) \cdot \square Rz = \square Rxy \cdot \square Rz = \square Rxyz = \square Rx \cdot \square Ryz = \square Rx \cdot (\square Ry \cdot \square Rz)$.
- Je-li $1 \in G$ neutrální prvek grupy G, pak pro libovolný prvek $\square Rx \in G/R$ platí $\square Rx \cdot \square R1 = \square Rx1 = \square Rx$ a také $\square R1 \cdot \square Rx = \square R1x = \square Rx$. Tedy $\square R1$ je neutrální prvek v G/R.
- Nechť $\square Rx \in G/R$ pro libovolné $x \in G$. Pak existuje $x^{-1} \in G$ a platí $\square Rx \cdot \square Rx^{-1} = \square Rxx^{-1} = \square R1$ a zároveň $\square Rx^{-1} \cdot \square Rx = \square Rx^{-1}x = \square R1$. Takže $(\square Rx)^{-1} = \square Rx^{-1}$.

Tedy $(G/R, \cdot)$ je grupa. □

Definice 4. 10. Grupa $(G/R, \cdot)$ z věty 4. 20. se nazývá faktorová grupa grupy G podle kongruence R.

Věta 4. 21. Nechť $(G, \cdot)$ je grupa, R kongruence v grupě G. Pak existuje normální podgrupa N v grupě G tak, že $(G/R, \cdot) = (G/N, \cdot)$.
Důkaz:
Nechť jsou splněny předpoklady věty. Definujme $N = \{x \in G; xR1\}$, kde 1 je neutrální prvek v grupě G.

1) Dokážeme, že N je normální podgrupa grupy G.
   - Zřejmě $N \neq \emptyset$ (neboť R je reflexivní, tedy $1R1$, tj. $1 \in N$) a $N \subseteq G$. Nechť $x, y \in N$ jsou libovolné prvky. Pak je $xR1$, $yR1$ a také $y^{-1}Ry^{-1}$. Díky podmínce kongruence odtud dostáváme $yy^{-1}R1y^{-1}$, neboli $1Ry^{-1}$, a vzhledem k symetričnosti relace R je též $y^{-1}R1$. Takže máme $xR1$ a zároveň $y^{-1}R1$, proto také $xy^{-1}R1$. To ovšem znamená, že $xy^{-1} \in N$, tedy N je podgrupou v G.
   - Nechť $g \in G$, $n \in N$ libovolné. Pak je $nR1$ a zároveň gRg, tedy máme $gnRg$ a také $g^{-1}Rg^{-1}$. Odtud dostáváme $gng^{-1}Rgg^{-1}$, neboli $gng^{-1}R1$. To ale znamená, že $gng^{-1} \in N$, takže N je normální podgrupa grupy G.

2) Ověříme rovnost $G/R = G/N$ (dokážeme inkluzi $G/R \subseteq G/N$, důkaz obrácené inkluze $G/N \subseteq G/R$ je obdobný).
   Nechť tedy A je libovolný prvek z rozkladu G/R. Pak existuje $x \in G$ tak, že $A = \square Rx$. Máme dokázat, že $A \in G/N$, tj. že existuje $g \in G$, pro něž $A = gN$. Položme $x = g$.
   - Nechť $t \in A = \square Rx$ je libovolný prvek. Potom je tRx a protože $x^{-1}Rx^{-1}$, dostáváme $x^{-1}tRx^{-1}x$, neboli $x^{-1}tR1$. To znamená, že $x^{-1}t \in N$, tedy existuje $n \in N$ takové, že $x^{-1}t = n$, takže $t = xn$. Proto je $t \in xN$, tudíž také $A \subseteq xN$.
   - Nechť $u \in xN$ je libovolný prvek. Potom existuje $n \in N$ tak, že $u = xn$, tedy $x^{-1}u = n$. Proto je $x^{-1}uR1$ a protože xRx, dostáváme $(xx^{-1})uRx$, neboli uRx. To znamená, že $u \in \square Rx = A$, tedy $xN \subseteq A$.

   Dostali jsme rovnost $A = xN$, takže $A \in G/N$. To ovšem znamená, že $G/R \subseteq G/N$. □

Věta 4. 22. Nechť $(G, \cdot)$ je grupa, N normální podgrupa v grupě G. Pak existuje kongruence R v grupě G taková, že $(G/R, \cdot) = (G/N, \cdot)$.
Důkaz:
Nechť jsou splněny předpoklady tvrzení. Definujme relaci R na G takto:
$(\forall\, x, y \in G)$ xRy, právě když $xy^{-1} \in N$.

1) Dokážeme, že R je kongruence v grupě G.

- Relace R je reflexivní, neboť pro každé $x \in G$ je $xx^{-1} = 1 \in N$, tedy xRx.
  Nechť $x, y \in G$ takové, že xRy, tj. $xy^{-1} \in N$. Poněvadž N je grupa, je $(xy^{-1})^{-1} = yx^{-1} \in N$, a tedy yRx. To znamená, že R je symetrická. Jestliže x, y, z jsou takové prvky z G, že xRy a zároveň yRz, dostáváme $xy^{-1} \in N$ a také $yz^{-1} \in N$. Tedy $xy^{-1}yz^{-1} = xz^{-1} \in N$, a proto xRz, čili R je tranzitivní. Tím jsme dokázali, že R je ekvivalence.
- Nechť x_1, x_2, y_1, y_2 jsou takové prvky z G, že platí x_1Rx_2 a současně y_1Ry_2, tedy $x_1x_2^{-1} \in N$ a také $y_1y_2^{-1} \in N$. Protože $y_1y_2^{-1} \in N$, prvek $x_2^{-1} \in G$ a N je normální podgrupa, existuje (viz lemma 4. 9.) prvek $n \in N$ tak, že $(y_1y_2^{-1})x_2^{-1} = x_2^{-1}n$. Potom $x_1(y_1y_2^{-1})x_2^{-1} = (x_1x_2^{-1})n \in N$, tedy $(x_1y_1)(y_2^{-1}x_2^{-1}) = (x_1y_1)(x_2y_2)^{-1} \in N$, neboli $x_1y_1Rx_2y_2$. Tím jsme dokázali, že R je kongruence.

2) Ověříme rovnost $G/N = G/R$ (dokážeme inkluzi $G/N \subseteq G/R$, obrácená inkluze se ověří analogicky).
   Nechť A je libovolný prvek, pro nějž platí $A \in G/N$. Pak existuje $g \in G$ tak, že $A = gN$.
   Máme dokázat, že $A \in G/R$, tj. že existuje $x \in G$, pro něž $A = \square Rx$. Položme $x = g$.
   - Nechť $t \in A = xN$ je libovolný prvek. Potom existuje $n \in N$ takové, že $t = xn$, tedy $x^{-1}t = n$, neboli $x^{-1}t1^{-1} = n$, takže $(x^{-1}t)1^{-1} \in N$. Proto je $x^{-1}tR1$ a protože xRx, dostáváme $(xx^{-1})tRx$, tj. tRx. To znamená, že $t \in \square Rx$, tedy $A \subseteq \square Rx$.
   - Nechť $u \in \square Rx$ je libovolný prvek. Potom je uRx a protože $x^{-1}Rx^{-1}$, dostáváme $x^{-1}uRx^{-1}x$, neboli $x^{-1}uR1$. To znamená, že $(x^{-1}u)1^{-1} \in N$, tj. $x^{-1}u \in N$. Takže existuje $n \in N$ takové, že $x^{-1}u = n$, čili $u = xn$. Proto je $u \in xN = A$, tudíž také $\square Rx \subseteq A$.

   Tedy dohromady $A = \square Rx$, takže $A \in G/R$ a inkluze $G/N \subseteq G/R$ je dokázána. □

Poznámka:
K definování kongruence nepotřebujeme žádné vlastnosti typické pro grupy, můžeme proto kongruenci R definovat (stejným způsobem) na libovolné struktuře $(G, *)$ s jednou binární operací a zavést faktorovou strukturu $(G/R, *)$.

2. 5. Permutační grupy

Nechť M je neprázdná množina. Permutací množiny M rozumíme každou bijekci M na M. Je-li M konečná, např. $M = \{1, 2,\ldots, n\}$, pak permutaci Π množiny M zapisujeme ve tvaru matice:

$$\Pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}, \text{ kde } \Pi(i) = j_i,\ i = 1, 2,\ldots, n.$$

Tento tvar se nazývá základní tvar permutace Π.

Je-li $(p_1, p_2,\ldots, p_n)$ libovolné pořadí prvků $1, 2,\ldots, n$ (tedy uspořádaná n-tice, v níž se každý z uvedených prvků vyskytuje právě jednou) a $\Pi(p_i) = q_i$, $i = 1, 2,\ldots, n$, můžeme permutaci Π zapsat v tzv. obecném tvaru:

$$\Pi = \begin{pmatrix} p_1 & p_2 & \ldots & p_n \\ q_1 & q_2 & \ldots & q_n \end{pmatrix}.$$

Prvek $i \in M$ se nazývá samodružný prvek permutace Π, jestliže $\Pi(i) = i$. V opačném případě se jedná o prvek nesamodružný.

- Permutace I na množině M se nazývá identická permutace, právě když každý prvek množiny M je samodružným prvkem permutace I, tj. $I = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$.
- Permutaci $\Pi^{-1} = \begin{pmatrix} q_1 & q_2 & \ldots & q_n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix}$ nazýváme inverzní permutací k permutaci $\Pi = \begin{pmatrix} p_1 & p_2 & \ldots & p_n \\ q_1 & q_2 & \ldots & q_n \end{pmatrix}$.
- Jsou-li $\Pi_1 = \begin{pmatrix} p_1 & p_2 & \ldots & p_n \\ q_1 & q_2 & \ldots & q_n \end{pmatrix}$ a $\Pi_2 = \begin{pmatrix} q_1 & q_2 & \ldots & q_n \\ r_1 & r_2 & \ldots & r_n \end{pmatrix}$ permutace množiny M, pak permutaci $\Pi = \begin{pmatrix} p_1 & p_2 & \ldots & p_n \\ r_1 & r_2 & \ldots & r_n \end{pmatrix}$ nazýváme součinem (složením) permutací Π_1, Π_2 a píšeme $\Pi_1 \cdot \Pi_2$ nebo $\Pi_1 \circ \Pi_2$. Násobení permutací je asociativní a není komutativní, neboť skládání zobrazení je vždy asociativní operace, která však není obecně komutativní.

Věta 5. 1. Množina všech permutací množiny $M = \{1, 2,\ldots, n\}$ tvoří spolu s operací násobení permutací nekomutativní grupu řádu $n!$, která se nazývá symetrická grupa n prvků a značí se symbolem S_n.
Důkaz:
Množina S_n je spolu s operací násobení zřejmě nekomutativní grupa. Vztah $|S_n| = n!$ se ověří úplnou indukcí podle n. □

Definice 5. 1. Nechť $p_1, p_2,\ldots, p_k$ je posloupnost různých prvků množiny $M = \{1, 2,\ldots, n\}$, $k \geq 2$. Permutaci $\Pi \in S_n$ takovou, že $\Pi(p_1) = p_2$, $\Pi(p_2) = p_3,\ldots, \Pi(p_{k-1}) = p_k$, $\Pi(p_k) = p_1$, $\Pi(p) = p$ pro každé $p \in M - \{p_1, p_2,\ldots, p_k\}$, nazýváme cyklickou permutací, resp. cyklem délky k a značíme $(p_1, p_2,\ldots, p_k)$; tedy $\Pi = (p_1, p_2,\ldots, p_k)$. Cykly délky 2 se nazývají transpozice na M. Říkáme, že dva cykly $(p_1, p_2,\ldots, p_k)$ a $(q_1, q_2,\ldots, q_l)$ jsou nezávislé, když $\{p_1, p_2,\ldots, p_k\} \cap \{q_1, q_2,\ldots, q_l\} = \emptyset$. Konečná množina cyklů se považuje za nezávislou, jsou-li každé dva cykly této množiny nezávislé. V opačném případě hovoříme o závislých cyklech.

Lemma 5. 2. Nechť $\Pi = (p_1, p_2,\ldots, p_k) \in S_n$. Pak platí:

1) $\Pi = (p_i, p_{i+1},\ldots, p_k, p_1,\ldots, p_{i-1})$ pro každé $i = 1, 2,\ldots, k$.
2) $\Pi^{-1} = (p_k, p_{k-1},\ldots, p_2, p_1)$.

Důkaz:

1), 2) Jedná se o bezprostřední důsledek definice 5. 1. □

Věta 5. 3. Součin nezávislých cyklů z S_n nezávisí na jejich pořadí.

Důkaz:

Uvažujme součin $\Pi_1 \cdot \Pi_2 \cdot\ldots\cdot \Pi_m$, kde $\Pi_1, \Pi_2,\ldots, \Pi_m \in S_n$ jsou nezávislé cykly. To ovšem znamená, že žádné dva z těchto cyklů nepřemisťují současně ten samý prvek, neboli permutace Π_i ponechává na místě ty prvky, na které působí permutace Π_j, $i \neq j$, $i, j = 1, 2,\ldots, m$, a naopak, každá permutace Π_j ponechává na místě ty prvky, na které působí Π_i. Tedy na umístění permutace Π_i v součin nezáleží. □

Věta 5. 4. Každou neidentickou permutaci Π na množině $M = \{1, 2,\ldots, n\}$ lze rozložit až na pořadí jednoznačně v součin nezávislých cyklů, jež jsou délky větší než jedna.

Důkaz: Viz [7].

Věta 5. 5. Každou permutaci Π na množině $M = \{1, 2,\ldots, n\}$ ($n \geq 2$) lze rozložit v součin transpozic.

Důkaz:

Libovolný cyklus můžeme rozložit jako $(p_1, p_2,\ldots, p_k) = (p_1, p_k)\cdot(p_1, p_{k-1})\cdot\ldots\cdot(p_1, p_3)\cdot(p_1, p_2)$ ($k \geq 2$). Je-li nyní $\Pi \neq I$, použijeme větu 5. 4., a tedy danou permutaci můžeme napsat jako součin rozkladů všech jejích cyklů. Identickou permutaci I můžeme zapsat ve tvaru $I = (p, q)\cdot(p, q)$, kde (p, q) je libovolná dvojice různých prvků z M. □

Definice 5. 2. Nechť Π je permutace množiny $M = \{1, 2,\ldots, n\}$. Říkáme, že dvojice (p, q) různých prvků z M představuje inverzi permutace Π, jestliže $(p - q)\cdot(\Pi(p) - \Pi(q)) < 0$; tedy je-li např. $\Pi(p) > \Pi(q)$ a zároveň $p < q$. Permutace Π se nazývá sudá nebo lichá podle toho, má-li sudý nebo lichý počet inverzí. Mluvíme pak o paritě permutace. Značí-li t počet inverzí permutace Π, pak definujeme $\operatorname{sgn}\Pi = (-1)^t$. Tedy, je-li sudá permutace, máme $\operatorname{sgn}\Pi = 1$, kdežto $\operatorname{sgn}\Pi = -1$, jakmile Π je permutace lichá; $\operatorname{sgn}\Pi$ (čteme signum) nazýváme znaménko permutace Π.

Poznámka:

1) Parita permutace je určena jednoznačně.
2) Grupa S_n má právě $\frac{n!}{2}$ sudých a $\frac{n!}{2}$ lichých permutací.

Věta 5. 6. Nechť $\Pi_1, \Pi_2 \in S_n$. Potom platí:

1) $\operatorname{sgn}(\Pi_1 \cdot \Pi_2) = \operatorname{sgn}\Pi_1 \cdot \operatorname{sgn}\Pi_2$,
2) $\operatorname{sgn}\Pi_1 = \operatorname{sgn}\Pi_1^{-1}$.

Důkaz: Viz [7].

Poznámka:

Podle definice 5. 2. a věty 5. 6. 1) je tedy součin dvou sudých nebo dvou lichých permutací sudá permutace, součin sudé a liché permutace (v libovolném pořadí) je lichá permutace.

Lemma 5. 7. Každá transpozice je lichou permutací.
Důkaz:
Nechť $\Pi = (p, q)$ je transpozice, kde p, q jsou různé prvky z M. Jelikož $(p, q) = (q, p)$, lze předpokládat, že $p < q$. Je-li $q = p + 1$, je dvojice $\{p, p + 1\}$ jedinou dvojicí představující inverzi permutace Π. Nechť $p + 1 < q$. V tomto případě dvojice $\{p, p + 1\}$, $\{p, p + 2\}$,…, $\{p, q\}$ a $\{p + 1, q\}$,…, $\{q - 1, q\}$ dávají množinu všech dvojic představujících inverzi permutace $\Pi = (p, q)$. Je jich celkem $(q - p) + (q - p) - 1$, což je liché číslo. □

Věta 5. 8. Permutace $\Pi \in S_n$ je sudá nebo lichá podle toho, zda je součinem sudého nebo lichého počtu transpozic. Je-li $\Pi = (p_1, p_2,\ldots, p_k)$ cyklus délky k, potom $\operatorname{sgn} \Pi = (-1)^{k-1}$.
Důkaz:
Podle věty 5. 5. lze permutaci Π rozložit alespoň jedním způsobem ve tvaru součinu transpozic $\Pi = \Pi_1 \cdot \Pi_2 \cdot \ldots \cdot \Pi_r$. Užitím lemmatu 5. 7. a věty 5. 6. 1) dostáváme $\operatorname{sgn} \Pi = (-1)^r$, z čehož plyne první část věty. Je-li $\Pi = (p_1, p_2,\ldots, p_k)$, potom $\Pi = (p_1, p_k)\cdot(p_1, p_{k-1})\cdot\ldots\cdot(p_1, p_2)$, a odtud $\operatorname{sgn} \Pi = (-1)^{k-1}$. □

Věta 5. 9. Množina A_n všech sudých permutací množiny $M = \{1, 2,\ldots, n\}$, $n \geq 2$, tvoří podgrupu symetrické grupy S_n indexu 2 (tedy je to normální podgrupa).
Důkaz:
Množina A_n je uzavřená vzhledem k operaci „·“, neboť součin dvou sudých permutací je opět sudá permutace, a tedy prvek množiny A_n. Asociativnost je dědičná vlastnost, identická permutace I obsahuje 0 inverzí, je tedy sudá a patří do A_n. Inverzní permutace k sudé permutaci je také sudá. Tedy A_n je podgrupa S_n. Jelikož sudých permutací je polovina, je A_n řádu $\frac{n!}{2}$ a indexu 2, a tedy podle věty 4. 11. je normální podgrupou grupy S_n. □

Definice 5. 3. Podgrupa A_n grupy S_n se nazývá alternující grupa permutací stupně n (nebo též alternující grupa n prvků). Jistě $A_1 = S_1$.

Věta 5. 10. Je-li $n \geq 2$, pak množina transpozic $\{(1, p); p = 2,\ldots, n\}$ je množinou generátorů symetrické grupy S_n. Je-li $n \geq 3$, pak množina cyklů délky 3 $\{(1, 2, p); p = 3,\ldots, n\}$ je množina generátorů alternující grupy A_n.
Důkaz:
Každou transpozici (p, q) je možno vyjádřit ve tvaru $(p, q) = (1, p)\cdot(1, q)\cdot(1, p)$. Odtud na základě věty 5. 5. již dostáváme první část věty. Obraťme se nyní k alternující grupě A_n. Podle věty 5. 8. lze každou sudou permutaci zapsat jako součin sudého počtu transpozic. Přitom $(p, q)\cdot(r, s) = (p, q, r)\cdot(q, r, s)$ a $(q, r)\cdot(p, q) = (p, r, q)$, takže množina všech cyklů délky 3 je množina generátorů pro A_n. Jelikož $(p, q, r) = (1, r, p)\cdot(1, p, q)$ a konečně $(1, p, q) = (1, 2, q)\cdot(1, 2, p)\cdot(1, 2, p)$, plyne odtud druhé tvrzení. □

Lemma 5. 11. Nechť H je podgrupa symetrické grupy S_n. Pak buď $H \subseteq A_n$, nebo je H sudého řádu a obsahuje týž počet lichých permutací jako sudých.
Důkaz: Viz [7].

Věta 5. 12. Permutace Π_1, Π_2 jsou konjugované v grupě S_n právě tehdy, když mají stejný počet cyklů každé délky.
Důkaz: Viz [6].

Lemma 5. 13. Je-li permutace $\Pi \in S_n$ k-členný cyklus, potom $k = o(\Pi)$.
Důkaz:
Nechť $\Pi = (p_1, p_2, \ldots, p_k)$. Ukážeme, že $\Pi^k = I$, kde k je nejmenší kladné celé číslo s touto vlastností:

$$\Pi(p_k) = p_1,\ \Pi^2(p_k) = \Pi(p_1) = p_2,\ \Pi^3(p_k) = \Pi(p_2) = p_3, \ldots,\ \Pi^{k-1}(p_k) = \Pi(p_{k-2}) = p_{k-1},$$
$$\Pi^k(p_k) = \Pi(p_{k-1}) = p_k .$$

Z poslední rovnosti dostáváme $\Pi^k = I$, což znamená, že $o(\Pi) = k$. □

Věta 5. 14. Řád permutace Π v grupě S_n, která je součinem navzájem nezávislých cyklů, je roven nejmenšímu společnému násobku délek jejích cyklů.
Důkaz:
Nechť $\Pi = \Pi_1 \cdot \Pi_2 \cdot \ldots \cdot \Pi_m$, kde $\Pi_1, \Pi_2, \ldots, \Pi_m \in S_n$ jsou nezávislé cykly, Π_i je délky k_i, $i = 1,2,\ldots, m$. Podle lemmatu 5. 13. je $o(\Pi_i) = k_i$, $\Pi_i^{k_i} = I$ a hledáme nejmenší kladné celé číslo n takové, že $\Pi^n = I$: $\Pi^n = (\Pi_1 \cdot \Pi_2 \cdot \ldots \cdot \Pi_m)^n = \Pi_1^n \cdot \Pi_2^n \cdot \ldots \cdot \Pi_m^n = I$, tedy $\Pi_1^n = I$, $\Pi_2^n = I, \ldots, \Pi_m^n$. Odtud dostáváme, že $k_i \mid n$ pro $i = 1,2,\ldots, m$. To ovšem znamená, že $n = nsn(k_1, k_2, \ldots, k_m)$. □

Poznámka:
Nejsou-li cykly nezávislé, tak nemusí být zaměnitelné a řád permutace, která je jejich součinem, se nemusí rovnat nejmenšímu společnému násobku jejich délek.

Věta 5. 15. Pro $n \geq 5$ je alternující grupa A_n jednoduchá.
Důkaz: Viz [5].

Věta 5. 16. (**Cayleyho**) Každá konečná grupa $(G, \cdot)$ řádu n je izomorfní s jistou podgrupou symetrické grupy S_n (neboli grupu $(G, \cdot)$ lze izomorfně vnořit do grupy S_n).
Důkaz:
Mějme dánu grupu $(G, \cdot)$ řádu n. Její prvky označme $a_1, a_2, \ldots, a_n$. Pro každé $x \in G$ označme F_x zobrazení G do G, které každému prvku $a \in G$ přiřazuje prvek ax, tj. $(\forall a \in G)\ F_x(a) = ax$. Takové zobrazení nazveme projekce grupy G (určená prvkem x). Protože v G lze krátit libovolným prvkem, je každá projekce F_x prosté zobrazení (pro libovolné prvky $a, b, x \in G$ platí: je-li $F_x(a) = F_x(b)$, pak $ax = bx$, a tedy $a = b$). Protože G je struktura s dělením, je F_x zobrazení G na G (pro všechna $b, x \in G$ existuje $a \in G$ tak, že $ax = b$, tedy $F_x(a) = b$). To znamená, že pro každé $x \in G$ je projekce F_x vlastně permutace množiny G, kterou díky označení prvků z G můžeme zapsat též takto:

$$F_x = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_1x & a_2x & \ldots & a_nx \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_{i1} & a_{i2} & \ldots & a_{in} \end{pmatrix},$$ kde pro $k = 1, 2, \ldots, n$ je $a_{ik} = a_kx$, tedy

a) každá projekce grupy G definuje jisté pořadí $(i_1, i_2, \ldots, i_n)$ čísel $1, 2, \ldots, n$.

Jsou-li x, y různé prvky grupy G, je $F_x(1) = x \neq F_y(1) = y$, kde 1 je jednotkový prvek grupy G. Odtud ihned plyne, že

b) různé prvky grupy G určují různé projekce grupy G (a tedy i pořadí definovaná těmito projekcemi jsou různá).

Díky asociativnosti grupy $(G, \cdot)$ snadno ukážeme, že

c) složení $F_x \cdot F_y$ projekcí F_x a F_y grupy G je opět projekce grupy G, přičemž platí:
$(\forall\, x, y \in G)\ F_x \cdot F_y = F_{xy}$.
K tomuto účelu zvolíme libovolné prvky $x, y, a \in G$ a postupně ukážeme:
$(F_x \cdot F_y)(a) = F_y(F_x(a)) = F_y(ax) = (ax)y = a(xy) = F_{xy}(a)$.
Protože a je libovolný prvek grupy G, dostáváme odtud ihned platnost celého tvrzení c).

Definujme nyní zobrazení φ: $G \longrightarrow S_n$, jež každému prvku $x \in G$ přiřadí permutaci

$\varphi(x) = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, kde $(i_1, i_2, \dots, i_n)$ je pořadí definované projekcí F_x podle a).

Z b) ihned plyne, že φ je prosté zobrazení množiny G do symetrické grupy S_n. Stačí tedy ověřit, že φ má vlastnost homomorfismu. Nechť x, y jsou libovolné prvky z G a nechť

$\varphi(x) = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, $\varphi(y) = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$, takže pro odpovídající projekce F_x, F_y platí $F_x(a_k) = a_{ik}$, $F_y(a_k) = a_{jk}$, $k = 1, 2, \dots, n$.

Pak dostáváme $F_{xy}(a_k) = (F_x \cdot F_y)(a_k) = F_y(F_x(a_k)) = F_y(a_{ik}) = a_{j_{ik}}$, takže

$\varphi(xy) = \begin{pmatrix} 1 & 2 & \dots & n \\ j_{i_1} & j_{i_2} & \dots & j_{i_n} \end{pmatrix}$. To však je permutace složená z permutací $\varphi(x)$ a $\varphi(y)$, neboť

$\varphi(x) \cdot \varphi(y) = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ j_{i_1} & j_{i_2} & \dots & j_{i_n} \end{pmatrix}$.

Tedy $\varphi(xy) = \varphi(x) \cdot \varphi(y)$, čímž je věta dokázána. □

Poznámka:

Budeme-li permutací rozumět prosté zobrazení jakékoliv (i nekonečné) množiny na sebe, můžeme právě dokázanou větu vyslovit v obecnějším tvaru, což ilustruje následující věta.

Věta 5. 17. Libovolná grupa $(G, \cdot)$ je izomorfní s jistou podgrupou grupy všech permutací množiny G.

Poznámka:

Každá podgrupa symetrické grupy S_n se nazývá permutační grupa. Permutační grupou se však nazývá i každá podgrupa permutací nekonečné množiny.

Věta 5. 18. Nechť $(G, \cdot)$ je struktura s krácením, s dělením a s jednotkovým prvkem. Potom $(G, \cdot)$ je asociativní, právě když skládání zobrazení je operací v množině všech projekcí F_x struktury $(G, \cdot)$.

Důkaz:

Nechť struktura $(G, \cdot)$ je s krácením, s dělením a s jednotkovým prvkem.

„$\Longrightarrow$“: Předpokládejme, že $(G, \cdot)$ je asociativní. Pak G je grupou a podle bodu c) důkazu věty 5. 16. (či – v případě nekonečné množiny G – analogicky podle věty 5. 17.) tvrzení platí.

„$\Longleftarrow$“: Předpokládejme, že skládání zobrazení je operací v množině všech projekcí v G. Pak k libovolným prvkům $x, y \in G$ musí existovat $z \in G$ takové, že $F_x \cdot F_y = F_z$, neboli $(F_x \cdot F_y)(a) = F_z(a)$ pro každé $a \in G$. Podle definice skládání zobrazení a definice projekce pak pro jednotkový prvek 1 struktury G dostáváme $(F_x \cdot F_y)(1) = F_y(F_x(1)) = F_y(x) = xy$, $F_z(1) = z$, tedy $xy = z$. To ovšem znamená, že $F_x \cdot F_y = F_{xy}$. Zvolme nyní libovolné prvky $x, y, z \in G$. Pak platí $x(yz) = F_{yz}(x) = (F_y \cdot F_z)(x) = F_z(F_y(x)) = F_z(xy) = (xy)z$. Tedy struktura $(G, \cdot)$ je asociativní. □

Poznámka:

V případě konečných struktur $(G, \cdot)$, jejichž operace je zadaná multiplikativní tabulkou, lze větu 5. 18. užít při ověřování asociativnosti operace „$\cdot$“.

2. 6. Grupy symetrií

Symetrie útvaru v rovině, resp. v prostoru, je shodné zobrazení roviny, resp. prostoru, které zobrazí daný objekt na sebe.
Grupa symetrií objektu je pak množina všech symetrií tohoto útvaru spolu s operací skládání symetrií.
Skutečně jde o grupu:

- složením dvou symetrií je opět symetrie,
- skládání zobrazení je asociativní,
- neutrálním prvkem je identické zobrazení I, které ponechává daný útvar na místě,
- symetrie jsou vlastně bijekce, proto musí ke každé symetrii nutně existovat symetrie inverzní.

Mezi grupami symetrií v rovině zaujímají význačné postavení tzv. dihedrální grupy, jimiž se budeme v dalším zabývat.

Dihedrální grupa D_n je grupa symetrií pravidelného n-úhelníku, tedy množina všech symetrií pravidelného n-úhelníku pro $n \geq 3$ spolu s operací skládání.

Při určování počtu symetrií pravidelného n-úhelníku je zřejmé, že máme

- n rotací: pravidelný n-úhelník lze otočit o úhel $\frac{2k\pi}{n}$, kde $k = 0,\ldots, n-1$, okolo svého středu tak, aby se zobrazil opět sám na sebe (pro $k = 0$ jde o identickou symetrii);
- n osových souměrností, a to jak pro liché, tak i sudé n:
  - liché n:
    - osy procházející každým vrcholem a středem protilehlé strany (celkem n),
  - sudé n:
    - osa pro každou dvojici protilehlých vrcholů (celkem $n/2$),
    - osa pro každou dvojici protilehlých středů stran (celkem $n/2$).

Tedy grupa D_n obsahuje minimálně $2n$ symetrií.

Označme vrcholy pravidelného n-úhelníku postupně čísly $1, 2,\ldots, n$. Každá symetrie je potom určena tím, jak zobrazuje vrcholy $1, 2,\ldots, n$ tohoto n-úhelníku.
Tedy dihedrální grupa D_n je podgrupou symetrické grupy S_n, neboť se skládá právě z těch permutací množiny $\{1, 2,\ldots, n\}$, které vzniknou, když čísly $1, 2,\ldots, n$ očíslujeme vrcholy pravidelného n-úhelníku a poté uvažujeme všechny jeho symetrie.

Označme:

- R … otočení (rotace) o úhel $\frac{2\pi}{n}$ okolo středu n-úhelníku v kladném směru
- O … osová souměrnost podle osy procházející vrcholem 1 (tzv. zrcadlení)

Rotace vždy zachovávají pořadí vrcholů i jejich směr.
Osová souměrnost naproti tomu vždy mění směr. Dvojí změnou pořadí dostaneme původní pořadí ($O \circ O = I$). Navíc složením libovolných dvou zrcadlení dostaneme rotaci.

Vezmeme-li rotaci R a osovou souměrnost O, pak celou grupu D_n vygenerujeme jen s jejich pomocí. Platí:

$$R^n = I,\ O^2 = I,\ R \circ O = O \circ R^{n-1} \text{ (tzv. definující relace).}$$

Symetrie R je řádu n, symetrie O a složená symetrie $R \circ O$ je řádu 2.

Jak již bylo řečeno, každá symetrie je určená tím, jak zobrazuje vrcholy 1, 2,…, n pravidelného n-úhelníku. Potom pokud nějakou symetrií zobrazíme vrchol 1 na vrchol i, symetrie buď zachovává cyklické pořadí vrcholů a je rovna R^{i-1}, nebo pořadí obrací a je rovna $O \circ R^{i-1}$. Proto řád grupy D_n je roven právě $2n$ a její prvky mají tvar:

$$I, R, R^2, R^3, \ldots, R^{n-1}, \; O, O \circ R, O \circ R^2, O \circ R^3, \ldots, O \circ R^{n-1}.$$

Tedy pro dihedrální grupu platí:

$D_n = [R, O] = \{ O^j \circ R^k; 0 \leq k < n, j \in \{0, 1\}, k \in \mathbb{Z}\}$.

Pro určení složení libovolných dvou symetrií grupy D_n používáme Cayleyho (multiplikativní) tabulku. Využíváme přitom faktu, že

$$R^n = I, O^2 = I \text{ a pro libovolné } i, 0 \leq i < n, \text{ je } R^i \circ O = O \circ R^{n-i}.$$

(Odvození:

$R^i \circ O = R^{i-1} \circ R \circ O = R^{i-1} \circ O \circ R^{n-1} = R^{i-2} \circ R \circ O \circ R^{n-1} = R^{i-2} \circ O \circ R^{n-1} \circ R^{n-1} =$
$= R^{i-2} \circ O \circ R^{n-2} = R^{i-3} \circ R \circ O \circ R^{n-2} = R^{i-3} \circ O \circ R^{n-1} \circ R^{n-2} = R^{i-3} \circ O \circ R^{n-3} = \ldots =$
$= R^{i-i} \circ O \circ R^{n-i} = O \circ R^{n-i}$.)

Při skládání symetrií postupujeme takto:

- $R^i \circ R^j = R^{(i+j) \bmod n}$, $0 \leq i, j < n$;
- $R^i \circ O \circ R^j = O \circ R^{(j-i) \bmod n}$ ($R^i \circ O \circ R^j = (R^i \circ O) \circ R^j = O \circ R^{n-i} \circ R^j = O \circ R^{-i} \circ R^j =$
  $= O \circ R^{j-i} = O \circ R^{(j-i) \bmod n}$), $0 \leq i, j < n$;
- $O \circ R^i \circ R^j = O \circ R^{(i+j) \bmod n}$, $0 \leq i, j < n$;
- $O \circ R^i \circ O \circ R^j = R^{(j-i) \bmod n}$ ($O \circ R^i \circ O \circ R^j = O \circ (R^i \circ O \circ R^j) = O \circ O \circ R^{(j-i) \bmod n} =$
  $= R^{(j-i) \bmod n}$), $0 \leq i, j < n$.

Poznámka:
$x \bmod n$ značí zbytek po dělení čísla x číslem n, tj. $0 \leq x \bmod n < n$.

Cayleyho tabulka pro grupu D_n:

$\circ$	I	R	R^2	…	R^{n-1}	O	$O \circ R$	$O \circ R^2$	…	$O \circ R^{n-1}$
I	I	R	R^2	…	R^{n-1}	O	$O \circ R$	$O \circ R^2$	…	$O \circ R^{n-1}$
R	R	R^2	$R^{3 \bmod n}$	…	I	$O \circ R^{n-1}$	O	$O \circ R$	…	$O \circ R^{n-2}$
R^2	R^2	$R^{3 \bmod n}$	$R^{4 \bmod n}$	…	R	$O \circ R^{n-2}$	$O \circ R^{n-1}$	O	…	$O \circ R^{n-3}$
⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮	…	⋮
R^{n-1}	R^{n-1}	I	R	…	R^{n-2}	$O \circ R$	$O \circ R^2$	$O \circ R^{3 \bmod n}$	…	O
O	O	$O \circ R$	$O \circ R^2$	…	$O \circ R^{n-1}$	I	R	R^2	…	R^{n-1}
$O \circ R$	$O \circ R$	$O \circ R^2$	$O \circ R^{3 \bmod n}$	…	O	R^{n-1}	I	R	…	R^{n-2}
$O \circ R^2$	$O \circ R^2$	$O \circ R^{3 \bmod n}$	$O \circ R^{4 \bmod n}$	…	$O \circ R$	R^{n-2}	R^{n-1}	I	…	R^{n-3}
⋮	⋮	⋮	⋮	…	⋮	⋮	⋮	⋮	…	⋮
$O \circ R^{n-1}$	$O \circ R^{n-1}$	O	$O \circ R$	…	$O \circ R^{n-2}$	R	R^2	$R^{3 \bmod n}$	…	I

Podgrupy D_n:
Každá podgrupa dihedrální grupy D_n je generována maximálně dvěma prvky. Dostáváme jen tři druhy podgrup grupy symetrií D_n pravidelného n-úhelníku:

- $\{I, R^j, R^{2j}, \ldots, R^{n-j}\}$ pro každé $j \mid n$,
- $\{I, O \circ R^i\}$ pro všechna $0 \leq i < n$,
- $\{I, R^k, R^{2k}, \ldots, R^{n-k}, O \circ R^h, O \circ R^{k+h}, O \circ R^{2k+h}, \ldots, O \circ R^{n-k+h}\}$ pro každé $k \mid n$ a každé $0 \leq h < k$.

Poznámka:
Podgrupy D_n viz [8].

2. 7. Homomorfismy grup

S homomorfním a izomorfním zobrazením algebraických struktur s jednou binární operací jsme se seznámili v 1. kapitole. Nyní se zaměříme čistě na homomofismy a izomorfismy grup.

Definice 7. 1. Nechť φ je homomorfismus grupy $(G, \cdot)$ na grupu $(H, \cdot)$, jejíž neutrální prvek je $1'$. Potom množina $Ker\ \varphi = J_\varphi = \{x \in G;\ \varphi(x) = 1'\}$ se nazývá jádro homomorfismu φ.

Definice 7. 2. Nechť φ je homomorfismus grupy $(G, \cdot)$ na grupu $(H, \cdot)$, K podmnožina v H. Množina $\varphi_{-1}(K) = \{x \in G;\ \varphi(x) \in K\}$ $(\subseteq G)$ se nazývá úplný vzor množiny K při homomorfismu φ. Je-li L podmnožina v G, pak množinu $\varphi(L) = \{\varphi(y) \in H;\ y \in L\}$ $(\subseteq H)$ nazýváme obrazem množiny L při homomorfismu φ. Obraz celé grupy G (tedy $\varphi(G)$) nazýváme obrazem homomorfismu φ a značíme $Im\ \varphi$.

Poznámka:
Z definice 7. 2. je zřejmé, že speciálně množina $\varphi_{-1}(\{1'\})$, kde $1'$ je neutrální prvek v H, je jádro homomorfismu φ.

Věta 7. 1. Nechť φ je homomorfismus grupy $(G, \cdot)$ na grupu $(H, \cdot)$. Pak φ je izomorfismus, právě když $Ker\ \varphi$ je jednoprvková množina, tj. když $Ker\ \varphi = \{1\}$, kde 1 je neutrální prvek grupy G.
Důkaz:
„$\Rightarrow$“: Předpokládejme, že φ je izomorfismus, tj. injektivní zobrazení. Jsou-li $x, y \in Ker\ \varphi$ libovolné prvky, pak $\varphi(x) = 1' = \varphi(y)$, kde $1'$ je neutrální prvek v H. Odtud již dostáváme rovnost $x = y$, neboť φ je injekce. Tedy $Ker\ \varphi$ je jednoprvková množina.

„$\Leftarrow$“: Předpokládejme, že φ není prosté zobrazení. Pak existují prvky $x, y \in G$ takové, že $x \neq y$ a zároveň $\varphi(x) = \varphi(y)$. Protože $x \neq y$, je také $xy^{-1} \neq 1$ (kdyby $xy^{-1} = 1$, pak $(xy^{-1})y = 1y$, neboli $x(y^{-1}y) = y$, takže $x = y$). Přitom ale platí $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi^{-1}(y) = \varphi(x)\varphi^{-1}(x) = 1'$. To znamená, že $Ker\ \varphi$ vedle prvku 1 obsahuje ještě prvek xy^{-1}, a není tedy jednoprvkovou množinou. □

Věta 7. 2. Nechť φ je homomorfismus grupy $(G, \cdot)$ na grupu $(H, \cdot)$. Pak platí:
1) Je-li K podgrupa v H, je $\varphi_{-1}(K)$ podgrupa v G.
2) Je-li $K \trianglelefteq H$, je $\varphi_{-1}(K) \trianglelefteq G$.
3) $Ker\ \varphi \trianglelefteq G$.
4) Je-li L podgrupa v G, je $\varphi(L)$ podgrupa v H.
5) $Im\ \varphi$ je podgrupa v H.
6) Je-li $L \trianglelefteq G$, je $\varphi(L) \trianglelefteq Im\ \varphi$.

Důkaz:
1) Předpokládejme, že K je podgrupa v H.
   - $\varphi_{-1}(K) \subseteq G$, $\varphi_{-1}(K) \neq \emptyset$ ($\varphi(1) = 1' \in K$, proto $1 \in \varphi_{-1}(K)$).
   - Jsou-li $x, y \in \varphi_{-1}(K)$ libovolné prvky, pak $\varphi(x), \varphi(y) \in K$, takže $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi^{-1}(y) \in K$. To znamená, že $xy^{-1} \in \varphi_{-1}(K)$.

   Tedy $\varphi_{-1}(K)$ je podgrupa v G.

2) Nechť $K \trianglelefteq H$. Podle 1) je $\varphi_{-1}(K)$ podgrupa grupy G. Jsou-li $g \in G$ a $x \in \varphi_{-1}(K)$ libovolné prvky, je $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) = \varphi(g)\varphi(x)\varphi^{-1}(g) \in K$, neboť $K \trianglelefteq H$, takže $gxg^{-1} \in \varphi_{-1}(K)$. Proto $\varphi_{-1}(K) \trianglelefteq G$.

3) Plyne okamžitě z 2).

4) Předpokládejme, že L je podgrupa v G.
   - $\varphi(L) \subseteq H$, $\varphi(L) \neq \emptyset$ ($1 \in L$, proto $\varphi(1) = 1' \in \varphi(L)$).
   - Jsou-li $x, y \in \varphi(L)$ libovolné prvky, pak existují $x_1, y_1 \in L$ tak, že $x = \varphi(x_1)$, $y = \varphi(y_1)$. Odtud $x_1 y_1^{-1} \in L$, takže máme $xy^{-1} = \varphi(x_1)\varphi^{-1}(y_1) = \varphi(x_1)\varphi(y_1^{-1}) = \varphi(x_1 y_1^{-1}) \in \varphi(L)$.

   Tedy $\varphi(L)$ je podgrupa v H.

5) Plyne bezprostředně ze 4), stačí volit $L = G$.

6) Nechť $L \trianglelefteq G$. Podle 5) a 4) je $\varphi(L)$ podgrupa grupy $Im\ \varphi$. Jsou-li $g \in Im\ \varphi$ a $x \in \varphi(L)$ libovolné, pak existují $g_1 \in G$, $x_1 \in L$ tak, že $g = \varphi(g_1)$, $x = \varphi(x_1)$. Potom je $gxg^{-1} = \varphi(g_1)\varphi(x_1)\varphi^{-1}(g_1) = \varphi(g_1)\varphi(x_1)\varphi(g_1^{-1}) = \varphi(g_1 x_1 g_1^{-1}) \in \varphi(L)$, neboť $g_1 x_1 g_1^{-1} \in L$. Tedy $\varphi(L) \trianglelefteq Im\ \varphi$. □

Věta 7. 3. Nechť $(G, \cdot)$ je grupa, N normální podgrupa grupy G. Pak faktorová grupa $(G/N, \cdot)$ je homomorfním obrazem grupy $(G, \cdot)$.

Důkaz:

Nechť jsou splněny předpoklady věty. Vytvořme faktorovou grupu G/N a definujme zobrazení:

$\varphi: G \longrightarrow G/N$

$(\forall\ x \in G)\ \ \varphi(x) = xN$

- φ je surjekce,
- $(\forall\ x, y \in G)\ \ \varphi(xy) = xyN = (xN)(yN) = \varphi(x)\varphi(y)$ – splněna podmínka homomorfismu.

Tedy φ je homomorfismus grupy G na grupu G/N. □

Poznámka:

1) Homomorfismus φ grupy G na její faktorovou grupu G/N (viz věta 7. 3.) se nazývá kanonický homomorfismus.
2) Jádro kanonického homomorfismu φ je totožné s normální podgrupou N grupy G: $Ker\ \varphi = \{x \in G;\ \varphi(x) = N\} = \{x \in G;\ xN = N\} = N$.

Věta 7. 4. (**věta o izomorfismu pro grupy**) Nechť grupa $(H, \cdot)$ je homomorfním obrazem grupy $(G, \cdot)$. Pak v grupě G existuje normální podgrupa N tak, že faktorová grupa $(G/N, \cdot)$ je izomorfní s grupou $(H, \cdot)$.

Důkaz:

1) Nechť φ je homomorfismus G na H. Položme $N = Ker\ \varphi$. Pak N je normální podgrupa (viz věta 7. 2. 3)), lze tedy vytvořit faktorovou grupu G/N.

2) Ukážeme, že předpis $(\forall\ xN \in G/N)\ \ \psi(xN) = \varphi(x)$ definuje izomorfismus G/N na H.
   - Nechť $xN, yN \in G/N$ libovolné takové, že $xN = yN$; pak podle věty 4. 3. máme $y^{-1}x \in N = Ker\ \varphi$, tedy $\varphi(y^{-1}x) = 1'$ ($1'$ je neutrální prvek v H). Protože φ je homomorfismus, dostáváme $\varphi(y^{-1})\varphi(x) = \varphi^{-1}(y)\varphi(x) = 1'$, takže $\varphi(x) = \varphi(y)$, tj. $\psi(xN) = \psi(yN)$. Výše uvedené vztahy jsou ekvivalentní, vyjdeme-li tedy z rovnosti $\psi(xN) = \psi(yN)$, dostaneme postupně až $xN = yN$. To ovšem znamená, že ψ je zobrazení, které je injektivní.
   - Zvolme libovolný prvek $y \in H$; protože φ je zobrazení G na H, existuje $x \in G$ tak, že $y = \varphi(x)$. Zároveň ale $\varphi(x) = \psi(xN)$, tudíž k prvku $y \in H$ existuje prvek $xN \in G/N$ tak, že $y = \psi(xN)$, tj. ψ je surjekce.
   - Zřejmě ψ je zobrazení celé množiny, tedy bijekce.

- Jsou-li $xN, yN \in G/N$ libovolné, je $\psi(xNyN) = \psi(xyN) = \varphi(xy) = \varphi(x)\varphi(y) = \psi(xN)\psi(yN)$ – splněna podmínka homomorfismu.

Tedy ψ je izomorfismus faktorové grupy G/N na grupu H. □

Vzhledem k tomu, co již bylo řečeno o souvislosti mezi normálními podgrupami a jádry homomorfismu, lze větu 7. 4. formulovat též takto:

Věta 7. 5. Nechť φ je homomorfismus grupy $(G, \cdot)$ na grupu $(H, \cdot)$, *Ker* φ jádro homomorfismu. Pak $(G/Ker\ \varphi, \cdot) \cong (H, \cdot)$.

Věta 7. 6. Nechť $(G, \cdot)$ je grupa a $g \in G$ je libovolný pevně zvolený prvek. Pak zobrazení $\varphi^g: G \longrightarrow G$ definované pro každé $x \in G$ předpisem $\varphi^g(x) = g^{-1}xg$ je automorfismus grupy G.
Důkaz:

- Pro libovolné $x, y \in G$ je $\varphi^g(xy) = g^{-1}(xy)g = (g^{-1}xg)(g^{-1}yg) = \varphi^g(x)\varphi^g(y)$, takže $\varphi^g: G \longrightarrow G$ je homomorfismus.
- Pro každé $x \in G$ je $\varphi^g(gxg^{-1}) = g^{-1}(gxg^{-1})g = x$, čili φ^g je surjekce.
- Zřejmě φ^g je zobrazení celé množiny.
- *Ker* $\varphi^g = \{x \in G;\ \varphi^g(x) = 1\} = \{x \in G;\ g^{-1}xg = 1\} = \{1\}$ (neboť $g^{-1}xg = 1$, právě když $xg = g$, tj. když $x = 1$). To znamená, že φ^g je injekce.

Tedy φ^g je automorfismus grupy G. □

Definice 7. 3. Je-li $(G, \cdot)$ grupa, pak se pro každý prvek $g \in G$ automorfismus φ^g nazývá vnitřní automorfismus grupy G určený prvkem g.

Poznámka:

1) Množinu všech automorfismů grupy G značíme symbolem *Aut G*, množinu všech vnitřních automorfismů symbolem *In G*.
2) Množina *Aut G* spolu s operací skládání zobrazení, tj. $(Aut\ G, \circ)$, je grupa.

Věta 7. 7. Je-li $(G, \cdot)$ grupa, pak množina *In G* spolu s operací skládání zobrazení je normální podgrupa grupy $(Aut\ G, \circ)$.
Důkaz:

1) Ukážeme, že *In G* je podgrupa *Aut G*.
   - Zřejmě *In G* $\subseteq$ *Aut G*; *In G* $\neq \emptyset$ (pro každé $x \in G$ je $1^{-1}x1 = x$, tj. $\varphi^1(x) = x$, čili $\varphi^1 = I \in In\ G$).
   - Pro každé tři prvky $g, h, x \in G$ máme $(\varphi^g \circ \varphi^h)(x) = \varphi^h(\varphi^g(x)) = \varphi^h(g^{-1}xg) = h^{-1}(g^{-1}xg)h = (h^{-1}g^{-1})x(gh) = (gh)^{-1}x(gh) = \varphi^{gh}(x)$, tedy $\varphi^g \circ \varphi^h = \varphi^{gh} \in In\ G$.
   - Neutrálním prvkem je $\varphi^1 = I \in In\ G$.
   - Asociativnost operace „$\circ$“ na množině *In G* plyne z téže vlastnosti na množině *Aut G* (dědičná vlastnost); nebo také z toho, že skládání zobrazení je obecně asociativní.
   - Je-li $g \in G$ libovolný prvek, existuje $g^{-1} \in G$ a platí $\varphi^g \circ \varphi^{g-1} = \varphi^{gg-1} = \varphi^1 = I$ a také $\varphi^{g-1} \circ \varphi^g = \varphi^{g-1g} = \varphi^1 = I$. Tedy $\varphi^{g-1} = (\varphi^g)^{-1} \in In\ G$.
2) Nechť $\alpha \in Aut\ G$, $\varphi^g \in In\ G$ libovolné. Pak pro každé $x \in G$ máme $(\alpha^{-1} \circ \varphi^g \circ \alpha)(x) = \alpha(\varphi^g(\alpha^{-1}(x))) = \alpha(g^{-1} \cdot \alpha^{-1}(x) \cdot g) = \alpha(g^{-1}) \cdot \alpha(\alpha^{-1}(x)) \cdot \alpha(g) = \alpha^{-1}(g) \cdot x \cdot \alpha(g) = \varphi^{\alpha(g)}(x)$; tedy $\alpha^{-1} \circ \varphi^g \circ \alpha = \varphi^{\alpha(g)} \in In\ G$. To však znamená, že *In G* $\trianglelefteq$ *Aut G*. □

Poznámka:

1) Zobrazení φ^g: $G \longrightarrow G$ definované pro každé $x \in G$ a pro pevně zvolené $g \in G$ předpisem $\varphi^g(x) = g^{-1}xg$ se také někdy nazývá konjugace (neboť prvky x, $\varphi^g(x)$ jsou konjugované v grupě G).
2) Je-li $(G, \cdot)$ komutativní grupa, pak $\varphi^g = I$ $((\forall\, g \in G)\ (\forall\, x \in G)\ \ \varphi^g(x) = g^{-1}xg = xg^{-1}g = x$, tj. $\varphi^g(x) = I(x))$.
3) Nechť H je podgrupa a φ endomorfismus grupy G. Říkáme, že podgrupa H je invariantní vůči homomorfismu φ, právě když pro každé $h \in H$ je $\varphi(h) \in H$, neboli $\varphi(H) \subseteq H$.
4) Podgrupa H je normální podgrupou grupy G, právě když H je invariantní vůči všem vnitřním automorfismům grupy G ($H \trianglelefteq G$, právě když pro každé $g \in G$ a každé $x \in H$ je $g^{-1}xg \in H$, tj. když $\varphi^g(x) \in H$).
5) Jestliže podgrupa H je invariantní vůči všem automorfismům grupy G, pak se nazývá charakteristická podgrupa grupy G. Je-li H invariantní vůči všem endomorfismům grupy G, pak se nazývá úplně charakteristická podgrupa grupy G.
6) Zřejmě každá úplně charakteristická podgrupa je již charakteristická a každá charakteristická je normální podgrupa.
7) Celá grupa G a jednotková podgrupa $\{1\}$ představují příklady úplně charakteristických podgrup.

Definice 7. 4. Nechť $(G, \cdot)$ je grupa. Množina $C(G) = \{g \in G;\ gx = xg$ pro každé $x \in G\}$ se nazývá centrum grupy G.

Věta 7. 8. Je-li $(G, \cdot)$ grupa, pak $C(G)$ je charakteristická podgrupa grupy G a každá podgrupa H taková, že $H \subseteq C(G)$, je normální v G.

Důkaz:

1) Ukážeme, že $C(G)$ je podgrupa v G.
   - Zřejmě $C(G) \subseteq G$; $C(G) \neq \emptyset$ (pro každé $x \in G$ je $1x = x1$, tj. $1 \in C(G)$).
   - Jsou-li $g, h \in C(G)$ libovolné, pak pro každé $x \in G$ je $gx = xg$ a $hx = xh$, a tedy také $xh^{-1} = h^{-1}x$. Potom však $(gh^{-1})x = g(h^{-1}x) = g(xh^{-1}) = (gx)h^{-1} = (xg)h^{-1} = x(gh^{-1})$, takže $gh^{-1} \in C(G)$, a podle věty 2. 4. je $C(G)$ podgrupa v G.
2) Je-li $g \in C(G)$ a $\varphi \in Aut\ G$, pak pro libovolné $y \in G$ existuje $x \in G$ tak, že $y = \varphi(x)$, načež dostáváme $\varphi(g)y = \varphi(g)\varphi(x) = \varphi(gx) = \varphi(xg) = \varphi(x)\varphi(g) = y\varphi(g)$. Odtud již je $\varphi(g) \in C(G)$, neboli $C(G)$ je invariantní vůči každému automorfismu $\varphi \in Aut\ G$. To ovšem znamená, že $C(G)$ je charakteristická podgrupa grupy G.
3) Jestliže H je podgrupa v G taková, že $H \subseteq C(G)$, pak pro každé $g \in G$ a $h \in H \subseteq C(G)$ je $gh = hg$, neboli $g^{-1}hg = h \in H$. Odtud $H \trianglelefteq G$. □

Věta 7. 9. Pro každou grupu $(G, \cdot)$ platí izomorfismus $G/C(G) \cong In\ G$.

Definice 7. 5. Je-li $(G, \cdot)$ grupa a x, y prvky z G, pak se prvek $x^{-1}y^{-1}xy$ nazývá komutátor (uspořádané) dvojice prvků x, y. Podgrupa G' grupy G generovaná množinou všech komutátorů se nazývá komutant grupy G.

Věta 7. 10. Pro každou grupu G je komutant G' úplně charakteristická podgrupa grupy G.

Věta 7. 11. Nechť G je komutativní grupa. Potom $C(G) = G$ a komutant $G' = \{1\}$.

Poznámka:
Důkazy vět 7. 9. – 7. 11. uvedeny v [7].

Zabývejme se nyní homomorfismy cyklických grup. Nechť tedy $G = [a]$ je cyklická grupa řádu n s neutrálním prvkem 1 a $H = [b]$ cyklická grupa řádu m s neutrálním prvkem $1'$.

1) Je-li $\varphi: G \longrightarrow H$ homomorfismus grup, pak platí:
   - $\varphi(a) = y$, kde $y \in H$,
   - $\varphi(1) = \varphi(a^n) = \varphi^n(a) = y^n = 1'$,
   - $(\forall\, x \in G)\ \ \varphi(x) = \varphi(a^l) = \varphi^l(a) = y^l$, kde $l \in \mathbb{Z}$,
   - $[\varphi(a)] \subset H$, nebo $[\varphi(a)] = H$ (v takovém případě je φ epimorfismus).

   Každý homomorfismus cyklické grupy je jednoznačně určen obrazem jejího generátoru. Chceme-li tedy nalézt všechny homomorfismy $\varphi: G \longrightarrow H$, musíme určit obraz generátoru a grupy G, tj. $\varphi(a) = y \in H$ tak, aby $y^n = 1'$. Pomocí $\varphi(a)$ pak pro každé $x \in G$ určíme $\varphi(x)$.

   Poznámka:
   Jestliže $m \mid n$, pak $n = mq$ a $y^n = y^{mq} = (y^m)^q = (1')^q = 1'$.
   Homomorfismů $\varphi: G \longrightarrow H$ je právě tolik, kolik prvků má grupa H.

2) Uvažujme endomorfismus $\varphi: G \longrightarrow G$.
   - $(\forall\, y \in G)\ \ y^n = (a^l)^n = a^{ln} = (a^n)^l = 1^l = 1$.

   Endomorfismů grupy G existuje právě tolik, kolik má grupa G prvků.

3) Nechť $\varphi: G \longrightarrow G$ je automorfismus. Obrazem generátoru musí být také generátor, takže máme:
   - $\varphi(a) = a^k$, kde $k \in \mathbb{Z}$, $nsd(k, n) = 1$ (viz věta 3. 11.),
   - $(\forall\, x \in G)\ \ \varphi(x) = \varphi(a^l) = \varphi^l(a) = (a^k)^l = a^{kl} = (a^l)^k = x^k$.

   Automorfismů grupy G je tedy právě tolik, kolik má grupa G generátorů.

4) Uvažujme endomorfismus $\varphi: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$, $\mathbb{Z} = [1] = [-1]$.
   - $\varphi(1) = y$, kde $y \in \mathbb{Z}$,
   - $(\forall\, x \in \mathbb{Z})\ \ \varphi(x) = \varphi(x \cdot 1) = x \cdot \varphi(1) = x \cdot y$.

   Endomorfismů grupy $\mathbb{Z}$ existuje nekonečně mnoho.

5) Nechť $\varphi: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$ je automorfismus.
   - $\varphi(1) = y$, $y \in \mathbb{Z}$, a zároveň y musí být generátor grupy $\mathbb{Z}$, proto máme $\varphi_1(1) = 1$ a $\varphi_2(1) = -1$,
   - $(\forall\, x \in \mathbb{Z})\ \ \varphi_1(x) = x \cdot 1 = x$, $\varphi_2(x) = x \cdot (-1) = -x$ (viz 4)).

   Tedy $Aut\ \mathbb{Z} = \{\varphi_1, \varphi_2\} \cong (\mathbb{Z}_2, \oplus)$.

3. Sbírka příkladů

3. 1. Algebraické struktury s jednou operací

3. 1. 1. Řešené příklady

Příklad 1. 1. 1:
Uveďte, kolika způsoby je možné definovat binární operaci v množině $X = \{a, b, c, d\}$.

Řešení:
Množina X je konečná (čtyřprvková), proto lze operaci v X zadat Cayleyho tabulkou. Počet všech navzájem různých binárních operací, jež lze definovat v množině X, je roven 4^{16}, neboť do každého z šestnácti polí tabulky můžeme zapsat libovolný ze čtyř prvků dané množiny.

Příklad 1. 1. 2:
Je dána množina M a předpis „$*$“. Rozhodněte, zda tento předpis definuje operaci v množině M, jestliže:

a) $M = \{-1, 0, 1\}$, $x * y = x + y$;
b) $M = \mathbb{N}$, $x * y = x - y$;
c) $M = \mathbb{R} - \{-1\}$, $x * y = x + y + xy$;
d) $M = \{x \in \mathbb{Z};\ x = 2k,\ k \in \mathbb{Z}\}$, $x * y = \frac{x + y}{2}$;
e) $M = \mathbb{R}$, $x * y = \operatorname{tg}(x + 2y)$.

Řešení:
Aby předpis „$*$“ definoval operaci v M, musí být množina M uzavřená vzhledem k „$*$“, tj. musí platit $x * y \in M$ pro každé $x, y \in M$.

a) Např. pro $x = 1 \in M$, $y = 1 \in M$ máme $x * y = 1 + 1 = 2 \notin M$, tedy předpis „$*$“ nedefinuje operaci v M.

b) Např. pro přirozená čísla $x = 2$, $y = 4$ máme $x * y = 2 - 4 = -2 \notin \mathbb{N}$, takže předpis „$*$“ nedefinuje operaci v $M = \mathbb{N}$.

c) Jsou-li $x, y \in \mathbb{R}$ libovolné, pak $xy \in \mathbb{R}$, a tudíž také $x + y + xy \in \mathbb{R}$. Protože ale uvažujeme množinu $M = \mathbb{R} - \{-1\}$, musíme ještě určit, pro která $x, y \in \mathbb{R}$ nastane $x * y = -1$:
$x * y = -1 \Leftrightarrow x + y + xy = -1 \Leftrightarrow x + y + xy + 1 = 0 \Leftrightarrow (x + 1) + y(1 + x) = 0 \Leftrightarrow$
$\Leftrightarrow (x + 1)\cdot(y + 1) = 0 \Leftrightarrow x = -1 \vee y = -1$. Tedy pokud je $x \neq -1$ a zároveň $y \neq -1$, je také $x * y \neq -1$, neboli $x * y \in \mathbb{R} - \{-1\}$. To ovšem znamená, že předpis „$*$“ definuje operaci v M.

d) Např. pro $x = 20 \in M$, $y = -2 \in M$ je $x * y = \frac{20 + (-2)}{2} = 9 \notin M$. Předpis „$*$“ tudíž nedefinuje operaci v M.

e) Protože $x * y = \operatorname{tg}(x + 2y) = \frac{\sin(x + 2y)}{\cos(x + 2y)}$, musí být $\cos(x + 2y) \neq 0$, tj. $x + 2y \neq \frac{\pi}{2} + k\pi$, kde $k \in \mathbb{Z}$. Např. ale pro $x = \frac{\pi}{2}$, $y = \pi$ dostáváme $x + 2y = \frac{\pi}{2} + 2\pi$, tedy předpis „$*$“ nedefinuje operaci v M.

Příklad 1. 1. 3:
Nechť operace „$\circ$“ je v množině $\mathbb{R}$ definovaná takto: $x \circ y = xy - 4x - 4y + 16$. Najděte všechna $x \in \mathbb{R}$ tak, že $(3 \circ x) \circ (3 \circ x) = 0$.

Řešení:
$3 \circ x = 3x - 12 - 4x + 16 = -x + 4$
$(3 \circ x) \circ (3 \circ x) = (-x + 4) \circ (-x + 4) = (-x + 4)^2 - 4(-x + 4) - 4(-x + 4) + 16 = 0$
$x^2 - 8x + 16 + 4x - 16 + 4x - 16 + 16 = 0$
$x^2 = 0 \Longrightarrow \underline{\underline{x = 0}}$.

Příklad 1. 1. 4:
Mějme strukturu (M, Δ), kde $M = \mathbb{Z} \times \mathbb{Z}$ a operace „Δ“ je definovaná takto:
$(\forall (x_1, y_1), (x_2, y_2) \in M)\ (x_1, y_1) \Delta (x_2, y_2) = (x_1 + x_2, y_1 \cdot y_2)$.
Zjistěte, zda struktura (M, Δ) je struktura s neutrálním prvkem.

Řešení:
Struktura (M, Δ) je s neutrálním prvkem, právě když platí:
$$(\exists (x_e, y_e) \in M)\ (\forall (x, y) \in M)\ (x, y) \Delta (x_e, y_e) = (x_e, y_e) \Delta (x, y) = (x, y).$$
Protože sčítání a násobení celých čísel je komutativní, stačí ověřit pouze jeden z těchto vztahů, např. $(x, y) \Delta (x_e, y_e) = (x, y)$. Musí tedy platit $(x + x_e, y \cdot y_e) = (x, y)$, takže dostáváme:
- $x + x_e = x$, tedy $x_e = 0$,
- $y \cdot y_e = y$, tedy $y_e = 1$ (pro $y \neq 0$).

Protože $y_e = 1$ pro nenulová y, musíme ještě ověřit, že uspořádaná dvojice $(0, 1)$ je neutrálním prvkem také pro $(x, 0) \in M$ libovolné:
- $(x, 0) \Delta (0, 1) = (x + 0, 0 \cdot 1) = (x, 0)$.

Tedy $(0, 1)$ je neutrálním prvkem struktury (M, Δ).

Poznámka:
Pokud bude daná struktura komutativní, budeme při určování dalších vlastností této struktury (již bez upozornění) vždy ověřovat pouze jeden z definičních vztahů dané vlastnosti.

Příklad 1. 1. 5:
V množině $G = \{a, b, c, d\}$ je dána operace „$\circ$“ tabulkou. Rozhodněte, zda je grupoid $(G, \circ)$ komutativní, resp. asociativní, resp. jestli má neutrální prvek.

a)

$\circ$	a	b	c	d
a	c	a	b	d
b	c	a	b	d
c	c	a	b	d
d	c	a	b	d

b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	b	d
c	c	c	b	d
d	d	d	d	d

Řešení:
a) Struktura $(G, \circ)$ není komutativní, není asociativní (např. $a \circ (b \circ c) = a \circ b = a$, ale $(a \circ b) \circ c = a \circ c = b$) a nemá neutrální prvek.

b) Struktura $(G, \circ)$ není komutativní, má neutrální prvek a. Protože G je strukturou s neutrálním prvkem a také s agresivním prvkem (= prvek d), stačí ověřit asociativnost operace „$\circ$“ pouze pro prvky b, c (viz kapitola 2. 1., poznámka na straně 14). Např. $b \circ (b \circ c) = b \circ b = c$, ale $(b \circ b) \circ c = c \circ c = b$, tedy G není asociativní.

Poznámka:
Jak poznáme vlastnosti konečné struktury, jejíž operace je zadaná Cayleyho tabulkou, je uvedeno v kapitole 2. 1., str. 14.

Příklad 1. 1. 6:
Je dán grupoid $(G, *)$. Rozhodněte, zda je tento grupoid komutativní, resp. asociativní, resp. zda má neutrální prvek, jestliže:

a) $G = \mathbb{Q}$, $x * y = (x - 1)\cdot(y - 1)$;

b) $G = \mathbb{R}^+$, $x * y = \frac{xy}{x^2 + y^2}$.

Řešení:

Nejprve vždy uvedeme vztah, který musí platit, aby byla struktura $(G, *)$ komutativní, resp. asociativní, resp. s neutrálním prvkem, a poté jej ověříme (takto budeme postupovat i v dalších příkladech na určování vlastností algebraických struktur).

a) $G = \mathbb{Q}$, $x * y = (x - 1)\cdot(y - 1)$

- Komutativnost:

  $(\forall x, y \in \mathbb{Q})\ x * y = y * x$

  $x * y = (x - 1)\cdot(y - 1) = (y - 1)\cdot(x - 1) = y * x$, tedy $(\mathbb{Q}, *)$ je komutativní.

- Asociativnost:

  $(\forall x, y, z \in \mathbb{Q})\ (x * y) * z = x * (y * z)$

  $L = (x * y) * z = [(x - 1)\cdot(y - 1)] * z = [(x - 1)\cdot(y - 1) - 1]\cdot(z - 1) =$

  $= (x - 1)\cdot(y - 1)\cdot(z - 1) - (z - 1)$

  $P = x * (y * z) = x * [(y - 1)\cdot(z - 1)] = (x - 1)\cdot[(y - 1)\cdot(z - 1) - 1] =$

  $= (x - 1)\cdot(y - 1)\cdot(z - 1) - (x - 1)$

  - např. pro $x = 1$, $y = 2$, $z = 3$ je $L \neq P$ ($L = -2$, $P = 0$), tj. $(\mathbb{Q}, *)$ není asociativní.

- Neutrální prvek:

  $(\exists e \in \mathbb{Q})\ (\forall x \in \mathbb{Q})\ x * e = x$

  $(x - 1)\cdot(e - 1) = x$

  $xe - e - x + 1 = x$

  $e(x - 1) = 2x - 1$

  $e = \frac{2x - 1}{x - 1}$ (pro $x \neq 1$)

  - protože neutrální prvek nesmí záviset na jiných prvcích dané struktury, nemá $(\mathbb{Q}, *)$ neutrální prvek.

b) $G = \mathbb{R}^+$, $x * y = \frac{xy}{x^2 + y^2}$

- Komutativnost:

  $(\forall x, y \in \mathbb{R}^+)\ x * y = y * x$

  $x * y = \frac{xy}{x^2 + y^2} = \frac{yx}{y^2 + x^2} = y * x$, tedy $(\mathbb{R}^+, *)$ je komutativní.

- Asociativnost:

  $(\forall x, y, z \in \mathbb{R}^+)\ (x * y) * z = x * (y * z)$

  $L = (x * y) * z = (\frac{xy}{x^2 + y^2}) * z = \frac{(\frac{xy}{x^2 + y^2})z}{(\frac{xy}{x^2 + y^2})^2 + z^2}$

  $P = x * (y * z) = x * (\frac{yz}{y^2 + z^2}) = \frac{x(\frac{yz}{y^2 + z^2})}{x^2 + (\frac{yz}{y^2 + z^2})^2}$

  - např. pro $x = 1$, $y = -1$, $z = 2$ je $L \neq P$ ($L = -\frac{4}{17}$, $P = -\frac{10}{29}$), tj. $(\mathbb{R}^+, *)$ není asociativní.

- Neutrální prvek:

  $(\exists e \in \mathbb{R}^+)\ (\forall x \in \mathbb{R}^+)\ x * e = x$

  $\frac{xe}{x^2 + e^2} = x$

  $xe = x(x^2 + e^2) \Longrightarrow e = x^2 + e^2$ (pro $x \neq 0$), tedy $(\mathbb{R}^+, *)$ nemá neutrální prvek.

Příklad 1. 1. 7:
Dokažte, že daná pologrupa $(G, *)$ má neutrální prvek. Dále pak nalezněte každý prvek z G, k němuž existuje prvek inverzní, a tento inverzní prvek určete, jestliže:

a) $G = \mathbb{Q}$, $x * y = x + y - xy$;
b) $G = \mathbb{Z}_7$, operace „$*$“ je násobení zbytkových tříd podle modulu 7, tj. operace „$\odot$“.

Řešení:
Obě struktury jsou komutativní.

a) $G = \mathbb{Q}$, $x * y = x + y - xy$
- Neutrální prvek:
$(\exists\, e \in \mathbb{Q})\ (\forall\, x \in \mathbb{Q})\ \ x * e = x$
$x + e - xe = x$
$e(1 - x) = 0$, tedy $e = 0$ (pro $x \neq 1$)
- musíme ještě ověřit, že 0 je neutrálním prvkem také pro $x = 1$:
$1 * 0 = 1 + 0 - 1 \cdot 0 = 1$, tedy $e = 0$ je neutrální prvek v $(\mathbb{Q}, *)$.

- Inverzní prvky:
$(\forall\, x \in \mathbb{Q})\ (\exists\, \overline{x} \in \mathbb{Q})\ \ x * \overline{x} = e$
$x + \overline{x} - x\overline{x} = 0$
$x + \overline{x}(1 - x) = 0$
$\overline{x} = -\frac{x}{1-x} = \frac{x}{x-1}$ (pro $x \neq 1$)
- tedy $(\forall\, x \in \mathbb{Q} - \{1\})\ \ \overline{x} = \frac{x}{x-1}$, k číslu $x = 1$ inverzní prvek neexistuje.

b) Sestavíme pro pologrupu $(\mathbb{Z}_7, \odot)$ Cayleyho tabulku, z níž určíme neutrální prvek a inverzní prvky:

$\odot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

- Neutrální prvek: $\overline{1}$.
- Inverzní prvky:
Prvek $\overline{1}$ je sám k sobě inverzní, prvek $\overline{6}$ je sám k sobě inverzní, dále pak navzájem inverzními prvky jsou dvojice: $\overline{2}$, $\overline{4}$; $\overline{3}$, $\overline{5}$.
K prvku $\overline{0}$ neexistuje inverzní prvek.

Příklad 1. 1. 8:
Je dána množina $G = \{a, b, c\}$ a částečná tabulka operace „$\circ$“ v G.

$\circ$	a	b	c
a	a	c	a
b	·	·	b
c	·	·	·

Doplňte tabulku tak, aby $(G, \circ)$
a) byl grupoid s neutrálním prvkem,
b) byl grupoid s inverzními prvky,
c) byl komutativní grupoid,
d) byla grupa.

Řešení:

a)

○	*a*	*b*	*c*
a	*a*	*c*	*a*
b	***a***	***b***	*b*
c	*a*	*b*	*c*

b)

○	*a*	*b*	*c*
a	*a*	*c*	*a*
b	*c*	***b***	*b*
c	*a*	*b*	*c*

c)

○	*a*	*b*	*c*
a	*a*	*c*	*a*
b	*c*	***a***	*b*
c	*a*	*b*	***b***

d) Tabulku nelze doplnit, neboť v každém řádku a v každém sloupci tabulky se každý prvek množiny G musí vyskytovat právě jednou (viz kapitola 2. 2., str. 20).

Poznámka:
Tučně zvýrazněny prvky, které můžeme volit libovolně.

Příklad 1. 1. 9:
Určete vlastnosti struktury $(M, *)$ a její typ, jestliže:

a) $M = \{0, 1, 2, 3, 4\}$, $x * y = |x - y|$;
b) $M = \mathbb{R}^+ - \{1\}$, $x * y = e^{(\ln x)(\ln y)}$;
c) $M = P(A)$, $A = \{1, 2, 3\}$, $X * Y = X \cap Y$, $X, Y \in P(A)$;
d) $M = \mathbb{Q}$, $x * y = 2x + 2y - 5$.

Řešení:

a) Sestavíme pro strukturu $(M, *)$ Cayleyho tabulku, ze které určíme její vlastnosti:

*	0	1	2	3	4
0	0	1	2	3	4
1	1	0	1	2	3
2	2	1	0	1	2
3	3	2	1	0	1
4	4	3	2	1	0

- M je uzavřená vzhledem k „$*$“.
- $(M, *)$ je komutativní, s neutrálním prvkem 0, s inverzními prvky (každý prvek je sám k sobě inverzní).
- $(M, *)$ není s krácením ani s (jednoznačným) dělením.

- Asociativnost:
$(\forall x, y, z \in M)\ (x * y) * z = x * (y * z)$
L $= (x * y) * z = |x - y| * z = ||x - y| - z|$, P $= x * (y * z) = x * |y - z| = |x - |y - z||$
- např. pro $x = 1$, $y = 2$, $z = 3$ je L $\neq$ P (L = 2, P = 0), tj. $(M, *)$ není asociativní.

Tedy $(M, *)$ je komutativní grupoid s neutrálním prvkem a s inverzními prvky.

b) $M = \mathbb{R}^+ - \{1\}$, $x * y = e^{(\ln x)(\ln y)}$
- Uzavřenost:
$(\forall x, y \in \mathbb{R}^+ - \{1\})\ x * y \in \mathbb{R}^+ - \{1\}$
Jsou-li $x, y \in \mathbb{R}^+$ libovolné, pak $\ln x, \ln y \in \mathbb{R}$, a tudíž také $(\ln x)(\ln y) \in \mathbb{R}$. Potom je ovšem $e^{(\ln x)(\ln y)} \in \mathbb{R}^+$. Protože uvažujeme množinu $\mathbb{R}^+ - \{1\}$, musíme určit, pro která $x, y \in \mathbb{R}^+$ nastane $x * y = 1$:
$x * y = 1 \Leftrightarrow e^{(\ln x)(\ln y)} = 1 \Leftrightarrow (\ln x)(\ln y) = 0 \Leftrightarrow \ln x = 0 \vee \ln y = 0 \Leftrightarrow x = 1 \vee \vee y = 1$. Pokud je $x \neq 1$ a současně $y \neq 1$, je také $x * y \neq 1$, neboli $x * y \in \mathbb{R} - \{1\}$; tedy uzavřenost platí.

- Asociativnost:
$(\forall x, y, z \in \mathbb{R}^+ - \{1\})\ (x * y) * z = x * (y * z)$
L $= (x * y) * z = [e^{(\ln x)(\ln y)}] * z = a * z = e^{(\ln a)(\ln z)} = e^{[(\ln x)(\ln y)](\ln z)} =$
$= e^{(\ln x)(\ln y)(\ln z)}$, kde $a = e^{(\ln x)(\ln y)}$.

P = $x * (y * z) = x * [e^{(\ln y)(\ln z)}] = x * b = e^{(\ln x)(\ln b)} = e^{(\ln x)[(\ln y)(\ln z)]} =$
$= e^{(\ln x)(\ln y)(\ln z)}$, kde $b = e^{(\ln y)(\ln z)}$.

Tedy L = P, takže $(\mathbb{R}^+ - \{1\}, *)$ je asociativní.

- Komutativnost:
  $(\forall x, y \in \mathbb{R}^+ - \{1\})\ x * y = y * x$
  $x * y = e^{(\ln x)(\ln y)} = e^{(\ln y)(\ln x)} = y * x$, tj. $(\mathbb{R}^+ - \{1\}, *)$ je komutativní.

- Neutrální prvek:
  $(\exists n \in \mathbb{R}^+ - \{1\})\ (\forall x \in \mathbb{R}^+ - \{1\})\ x * n = x$
  $e^{(\ln x)(\ln n)} = x$
  $(\ln x)(\ln n) = \ln x$
  $\ln n = 1$, tudíž $n = e$ (tj. Eulerovo číslo) je neutrální prvek v $(\mathbb{R}^+ - \{1\}, *)$

- Inverzní prvky:
  $(\forall x \in \mathbb{R}^+ - \{1\})\ (\exists \overline{x} \in \mathbb{R}^+ - \{1\})\ x * \overline{x} = n$
  $e^{(\ln x)(\ln \overline{x})} = e$
  $(\ln x)(\ln \overline{x}) = 1$
  $\ln \overline{x} = \frac{1}{\ln x}$, tedy $\overline{x} = e^{\frac{1}{\ln x}}$, tj. $(\mathbb{R}^+ - \{1\}, *)$ je struktura s inverzními prvky.

- Krácení:
  $(\forall x, y, z \in \mathbb{R}^+ - \{1\})\ x * z = y * z \Longrightarrow x = y$
  $x * z = y * z \Longrightarrow e^{(\ln x)(\ln z)} = e^{(\ln y)(\ln z)} \Longrightarrow (\ln x)(\ln z) = (\ln y)(\ln z) \Longrightarrow$
  $\Longrightarrow \ln x = \ln y \Longrightarrow x = y$, tj. $(\mathbb{R}^+ - \{1\}, *)$ je struktura s krácením.

- Dělení:
  $(\forall x, y \in \mathbb{R}^+ - \{1\})\ (\exists z \in \mathbb{R}^+ - \{1\})\ x * z = y$
  $e^{(\ln x)(\ln z)} = y$
  $(\ln x)(\ln z) = \ln y$
  $\ln z = \frac{\ln y}{\ln x}$, tedy $z = e^{\frac{\ln y}{\ln x}}$, tj. $(\mathbb{R}^+ - \{1\}, *)$ je struktura s dělením, a to s jednoznačným dělením (pro každé $x, y \in \mathbb{R}^+ - \{1\}$ existuje právě jedno $z \in \mathbb{R}^+ - \{1\}$ tak, že $x * z = y$).

Tedy $(\mathbb{R}^+ - \{1\}, *)$ je abelovská grupa.

Poznámka:
Protože grupa je struktura s krácením a s (jednoznačným) dělením, nemuseli jsme poslední dvě vlastnosti ověřovat.

c) $M = P(A)$, $A = \{1, 2, 3\}$, $X * Y = X \cap Y$, $X, Y \in P(A)$
- Uzavřenost:
  $(\forall X, Y \in P(A))\ X \cap Y \in P(A)$ – platí.

- Pro libovolné množiny $X, Y, Z \in P(A)$ platí asociativnost a komutativnost průniku, tj.
  $(X \cap Y) \cap Z = X \cap (Y \cap Z)$, $X \cap Y = Y \cap X$.

- Neutrální prvek:
  $(\exists E \in P(A))\ (\forall X \in P(A))\ X \cap E = X$
  $E = A$ je neutrálním prvkem v $P(A)$.

- Inverzní prvky:
  $(\forall X \in P(A))\ (\exists \overline{X} \in P(A))\ X \cap \overline{X} = A$
  - např. pro $X = \{1\}$ neexistuje inverzní prvek, tudíž $P(A)$ není s inverzními prvky.

- Krácení:
  $(\forall X, Y, Z \in P(A))\ \ X \cap Z = Y \cap Z \Longrightarrow X = Y$
  - neplatí např. pro $X = \{1, 2\}$, $Y = A$, $Z = \{1\}$, neboť $X \cap Z = Y \cap Z = Z$, přitom ale $X \neq Y$. Tedy $P(A)$ není s krácením.
- Dělení:
  $(\forall X, Y \in P(A))\ (\exists Z \in P(A))\ \ X \cap Z = Y$
  - neplatí např. pro $X = \{1\}$, $Y = A$, takže $P(A)$ není s (jednoznačným) dělením.
- $(\forall X \in P(A))\ \ X \cap \emptyset = \emptyset$, což znamená, že $\emptyset$ je agresivním prvkem v $P(A)$.

Tedy $(P(A), \cap)$ je komutativní monoid s agresivním prvkem.

d) $M = \mathbb{Q}$, $x * y = 2x + 2y - 5$
- Uzavřenost:
  $(\forall x, y \in \mathbb{Q})\ \ x * y \in \mathbb{Q}$
  Jsou-li $x, y \in \mathbb{Q}$ libovolné, pak $2x, 2y \in \mathbb{Q}$, a tudíž také $2x + 2y - 5 \in \mathbb{Q}$. Tedy množina $\mathbb{Q}$ je uzavřená vzhledem k operaci „$*$“.
- Asociativnost:
  $(\forall x, y, z \in \mathbb{Q})\ \ (x * y) * z = x * (y * z)$
  $L = (x * y) * z = (2x + 2y - 5) * z = 2(2x + 2y - 5) + 2z - 5 = 4x + 4y + 2z - 15$
  $P = x * (y * z) = x * (2y + 2z - 5) = 2x + 2(2y + 2z - 5) - 5 = 2x + 4y + 4z - 15$
  - např. pro $x = 1$, $y = -1$, $z = 0$ je $L \neq P$ ($L = -15$, $P = -17$), tj. $(\mathbb{Q}, *)$ není asociativní.
- Komutativnost:
  $(\forall x, y \in \mathbb{Q})\ \ x * y = y * x$
  $x * y = 2x + 2y - 5 = 2y + 2x - 5 = y * x$, tedy $(\mathbb{Q}, *)$ je komutativní.
- Neutrální prvek:
  $(\exists e \in \mathbb{Q})\ (\forall x \in \mathbb{Q})\ \ x * e = x$
  $2x + 2e - 5 = x$
  $2e = 5 - x$
  $e = \frac{5 - x}{2}$
  - tedy $(\mathbb{Q}, *)$ nemá neutrální prvek, a tudíž není ani strukturou s inverzními prvky.
- Krácení:
  $(\forall x, y, z \in \mathbb{Q})\ \ x * z = y * z \Longrightarrow x = y$
  $x * z = y * z \Longrightarrow 2x + 2z - 5 = 2y + 2z - 5 \Longrightarrow 2x = 2y \Longrightarrow x = y$, takže $(\mathbb{Q}, *)$ je struktura s krácením.
- Dělení:
  $(\forall x, y \in \mathbb{Q})\ (\exists z \in \mathbb{Q})\ \ x * z = y$
  $2x + 2z - 5 = y$
  $2z = y - 2x + 5$
  $z = \frac{y - 2x + 5}{2}$, tj. $(\mathbb{Q}, *)$ je struktura s (jednoznačným) dělením.

Tedy $(\mathbb{Q}, *)$ je komutativní kvazigrupa.

Příklad 1. 1. 10:
Nechť $G = \{S, P, L, Z\}$ je množina, kde prvky množiny G jsou povely: S – zůstaňte na místě, P – vpravo v bok, L – vlevo v bok, Z – čelem vzad. V množině G definujme operaci „$\circ$“ takto: $x \circ y = z$, kde z značí ten povel, jímž můžeme nahradit povely x, y provedené po sobě. Utvořte tabulku operace „$\circ$“ a určete typ struktury $(G, \circ)$.

Řešení:

○	*S*	*P*	*L*	*Z*
S	*S*	*P*	*L*	*Z*
P	*P*	*Z*	*S*	*L*
L	*L*	*S*	*Z*	*P*
Z	*Z*	*L*	*P*	*S*

- G je uzavřená vzhledem k „○“.
- $(G, \circ)$ je komutativní, s neutrálním prvkem S, s inverzními prvky: prvek S (Z) je sám k sobě inverzní, prvky P, L jsou navzájem inverzní.

Poznámka:
Dá se dokázat, že je-li operace „○“ komutativní, pak platí:

- pro každé $a \in G$ splňuje uspořádaná trojice (a, a, a) asociativnost operace „○“;
- jestliže pro každé $a, b, c \in G$ uspořádané trojice (a, b, c) a (b, a, c) splňují asociativnost operace „○“, pak také uspořádané trojice (a, c, b), (c, b, a), (b, c, a), (c, a, b) splňují asociativnost operace „○“;
- pro každé $a, b \in G$ splňuje uspořádaná trojice (a, b, a) asociativnost operace „○“;
- jestliže pro každé $a, b \in G$ uspořádaná trojice (a, a, b) splňuje asociativnost operace „○“, pak také uspořádaná trojice (b, a, a) splňuje asociativnost operace „○“.

Nemusíme tedy v případě asociativnosti ověřovat 3^3 definičních vztahů pro prvky P, L, Z, ale pouze tyto rovnosti:

- $(P \circ L) \circ Z = P \circ (L \circ Z) \Longrightarrow S \circ Z = P \circ P \Longrightarrow Z = Z$
- $(L \circ P) \circ Z = L \circ (P \circ Z) \Longrightarrow S \circ Z = L \circ L \Longrightarrow Z = Z$
- $(P \circ P) \circ L = P \circ (P \circ L) \Longrightarrow Z \circ L = P \circ S \Longrightarrow P = P$
- $(P \circ P) \circ Z = P \circ (P \circ Z) \Longrightarrow Z \circ Z = P \circ L \Longrightarrow S = S$
- $(L \circ L) \circ P = L \circ (L \circ P) \Longrightarrow Z \circ P = L \circ S \Longrightarrow L = L$
- $(L \circ L) \circ Z = L \circ (L \circ Z) \Longrightarrow Z \circ Z = L \circ P \Longrightarrow S = S$
- $(Z \circ Z) \circ P = Z \circ (Z \circ P) \Longrightarrow S \circ P = Z \circ L \Longrightarrow P = P$
- $(Z \circ Z) \circ L = Z \circ (Z \circ L) \Longrightarrow S \circ L = Z \circ P \Longrightarrow L = L$.

Tedy struktura $(G, \circ)$ je komutativní, asociativní, s neutrálním prvkem a s inverzními prvky, tj. abelovská grupa.

Příklad 1. 1. 11:
Je dán grupoid $(\mathbb{Z}^+, +)$ a podmnožina $H \subseteq \mathbb{Z}^+$. Rozhodněte, zda $(H, +)$ je podgrupoidem grupoidu $(\mathbb{Z}^+, +)$, je-li:

a) $H = \mathbb{Z}^+ - \{1, 2, 4, 5\}$;
b) $H = \mathbb{Z}^+ - \{1, 2, 5, 6\}$;
c) H je libovolná, neprázdná konečná podmnožina množiny $\mathbb{Z}^+$;
d) $H = \{x \in \mathbb{Z}^+; 3 \mid x \vee 7 \mid x\}$.

Řešení:
Množina H musí být uzavřená vzhledem k operaci „+“.

a) $H = \{3, 6, 7, 8, 9, 10, \ldots\}$; sečteme-li libovolné dva prvky z H, dostaneme opět prvek množiny H, tedy $(H, +)$ je podgrupoidem grupoidu $(\mathbb{Z}^+, +)$.

b) $H = \{3, 4, 7, 8, 9, 10, \ldots\}$; protože $3 \in H$, ale $3 + 3 = 6 \notin H$, není $(H, +)$ podgrupoidem grupoidu $(\mathbb{Z}^+, +)$.

c) Je-li např. $H = \{1, 2, 3\}$, pak $2, 3 \in H$, ale $2 + 3 = 5 \notin H$, takže $(H, +)$ není podgrupoidem $(\mathbb{Z}^+, +)$.

d) $H = \{3, 6, 7, 9, 12, 14, 15, 18, 21, \ldots\}$; tedy např. $6, 7 \in H$, ale $6 + 7 = 13 \notin H$, tudíž $(H, +)$ není podgrupoidem $(\mathbb{Z}^+, +)$.

Příklad 1. 1. 12:
V množině G je daná operace „$\cdot$“ tabulkou:

$\cdot$	a	b	c	d
a	a	c	c	a
b	b	b	c	a
c	b	c	b	a
d	a	b	b	a

V grupoidu $(G, \cdot)$ pak nalezněte všechny podgrupoidy, resp. všechny podpologrupy, resp. všechny podgrupy.

Řešení:

- Podgrupoidy:
  Existuje celkem patnáct neprázdných podmnožin množiny G. Musíme zjistit, které z nich jsou uzavřené vzhledem k operaci „$\cdot$“.
  Dostáváme: $(G_1, \cdot) = (\{a\}, \cdot)$, $(G_2, \cdot) = (\{b\}, \cdot)$, $(G_3, \cdot) = (\{b, c\}, \cdot)$, $(G_4, \cdot) = (\{a, d\}, \cdot)$, $(G_5, \cdot) = (\{a, b, c\}, \cdot)$, $(G_6, \cdot) = (G, \cdot)$.
- Podpologrupy:
  $(G_1, \cdot)$, $(G_2, \cdot)$, $(G_3, \cdot)$, $(G_4, \cdot)$ (splňují asociativnost operace „$\cdot$“, kdežto $(G_5, \cdot)$, $(G_6, \cdot)$ nejsou asociativní; např. $(a \cdot b) \cdot c = c \cdot c = b$, ale $a \cdot (b \cdot c) = a \cdot c = c$).
- Podgrupy:
  $(G_1, \cdot)$, $(G_2, \cdot)$, $(G_3, \cdot)$ ($(G_4, \cdot)$ není podgrupou, protože nemá neutrální prvek, tj. ani inverzní prvky).

Příklad 1. 1. 13:
Dokažte, že operace „$\oplus$“ a „$\odot$“ definované v množině $\mathbb{Z}_m$, $m \in \mathbb{Z}$, $m > 1$, předpisem:
$(\forall\, \overline{x}, \overline{y} \in \mathbb{Z}_m)\ \ \overline{x} \oplus \overline{y} = \overline{x + y},\ \ \overline{x} \odot \overline{y} = \overline{xy}$

a) nezávisí na volbě reprezentantů $(*)$; b) jsou asociativní a komutativní.

Řešení:

a) Předpokládejme, že $\overline{x_1} = \overline{x_2}$, $\overline{y_1} = \overline{y_2}$. Pak $x_1 = mq_1 + r$, $x_2 = mq_2 + r$, $y_1 = mt_1 + s$, $y_2 = mt_2 + s$, kde $0 \leq r, s < m$; $q_1, q_2, t_1, t_2 \in \mathbb{Z}$.
   Pak platí:
   - $x_1 + y_1 = m(q_1 + t_1) + (r + s),\ \ x_2 + y_2 = m(q_2 + t_2) + (r + s)$, takže $\overline{x_1 + y_1} = \overline{x_2 + y_2}$;
   - $x_1 y_1 = m(q_1 t_1 m + q_1 s + t_1 r) + rs,\ \ x_2 y_2 = m(q_2 t_2 m + q_2 s + t_2 r) + rs$, takže $\overline{x_1 y_1} = \overline{x_2 y_2}$.

   Tedy operace „$\oplus$“ a „$\odot$“ v $\mathbb{Z}_m$ nezávisí na volbě reprezentantů.

b) $(\forall\, \overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_m)$
   - $(\overline{x} \oplus \overline{y}) \oplus \overline{z} = \overline{x + y} \oplus \overline{z} = \overline{(x + y) + z} = \overline{x + (y + z)} = \overline{x} \oplus \overline{y + z} = \overline{x} \oplus (\overline{y} \oplus \overline{z})$
   - $\overline{x} \oplus \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} \oplus \overline{x}$
   - $(\overline{x} \odot \overline{y}) \odot \overline{z} = \overline{xy} \odot \overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x} \odot \overline{yz} = \overline{x} \odot (\overline{y} \odot \overline{z})$
   - $\overline{x} \odot \overline{y} = \overline{xy} = \overline{yx} = \overline{y} \odot \overline{x}$.

   Tedy operace „$\oplus$“ a „$\odot$“ v $\mathbb{Z}_m$ jsou asociativní a komutativní.

3. 1. 2. Příklady k procvičení

Příklad 1. 2. 1:
Je dána množina T a předpis „$\circ$“. Rozhodněte, zda tento předpis definuje operaci v množině T, jestliže:

a) $T = \{-1, 0, 1\}$, $x \circ y = xy$;
b) $T = \mathbb{Q}$, $x \circ y = \frac{2xy^2}{x^2 + y^3}$;
c) $T = \mathbb{R}$, $x \circ y = \sin(xy - 3x^3)$;
d) $T = \mathbb{R}$, $x \circ y = \operatorname{cotg}(3x + 2y)$.

Příklad 1. 2. 2:
Nechť operace „$*$“ je v množině $\mathbb{R}$ definovaná takto: $x * y = \frac{x + y}{x \cdot y}$. Najděte všechna $x \in \mathbb{R}$ tak, že $(x * 1) * (x * 1) = 0{,}4375$.

Příklad 1. 2. 3:
V množině $G = \{a, b, c, d\}$ je dána operace „$\circ$“ tabulkou. Rozhodněte, zda je grupoid $(G, \circ)$ komutativní, resp. asociativní, resp. jestli má neutrální prvek.

$\circ$	a	b	c	d
a	c	a	b	a
b	a	a	d	b
c	b	d	b	c
d	a	b	c	d

Příklad 1. 2. 4:
Je dán grupoid $(G, *)$. Rozhodněte, zda je tento grupoid komutativní, resp. asociativní, resp. zda má neutrální prvek, jestliže:

a) $G = \mathbb{R}$, $x * y = (x + y) \cdot (1 + xy)$;
b) $G = \mathbb{Z}$, $x * y = |x|$.

Příklad 1. 2. 5:
Dokažte, že daná pologrupa $(G, *)$ má neutrální prvek. Dále pak nalezněte každý prvek z G, k němuž existuje prvek inverzní, a tento inverzní prvek určete, jestliže:

a) $G = \mathbb{Z}$, $x * y = x + y - xy$;
b) $G = \mathbb{Z}_6$, operace „$*$“ je násobení zbytkových tříd podle modulu 6, tj. operace „$\odot$“.

Příklad 1. 2. 6:
Určete vlastnosti struktury $(M, *)$ a její typ, jestliže:

a) $M = \mathbb{N} - \{0\}$, $x * y = x^y$;
b) $M = \mathbb{R}^+$, $x * y = x^2 y^2$;
c) $M = \mathbb{R}^+$, $x * y = \sqrt{xy}$;
d) $M = P(A)$, $A = \{1, 2, 3\}$, $X * Y = X \cup Y$, $X, Y \in P(A)$.

Příklad 1. 2. 7:
V množině $G = \{a, b, c\}$, resp. $G = \{a, b, c, d\}$, je dána operace „$\circ$“ tabulkou. Určete typ algebraické struktury $(G, \circ)$, jestliže:

a)

$\circ$	a	b	c
a	a	b	c
b	b	c	b
c	c	c	b

b)

$\circ$	a	b	c	d
a	a	a	a	a
b	a	d	b	d
c	a	b	c	d
d	a	d	d	b

Příklad 1. 2. 8:
V množině G je daná operace „$\cdot$“ tabulkou:

$\cdot$	a	b	c	d
a	a	c	b	d
b	c	b	c	a
c	b	c	b	a
d	d	b	b	d

V grupoidu $(G, \cdot)$ pak nalezněte všechny podgrupoidy, resp. všechny podpologrupy, resp. všechny podgrupy.

3. 2. Základní vlastnosti grup

3. 2. 1. Řešené příklady

Příklad 2. 1. 1:
Je dán komutativní grupoid $(G, *)$. Rozhodněte, zda $(G, *)$ je komutativní grupou, jestliže:

a) $G = \mathbb{Q} - \{0\}$, $x * y = |x \cdot y|$;

b) $G = \{a + ib\sqrt{5};\ a, b \in \mathbb{Q} \wedge (a^2 + b^2) \neq 0\}$, operace „$*$“ je násobení komplexních čísel.

Řešení:

a) - Asociativnost:
$(\forall x, y, z \in G)\ (x * y) * z = x * (y * z)$
$L = (x * y) * z = |x \cdot y| * z = ||x \cdot y| \cdot z| = |x \cdot y \cdot z|$
$P = x * (y * z) = x * |y \cdot z| = |x \cdot |y \cdot z|| = |x \cdot y \cdot z|$
Tedy L = P, takže $(G, *)$ je asociativní.

- Neutrální prvek:
$(\exists e \in G)\ (\forall x \in G)\ x * e = x$
$|x \cdot e| = x$, tj. např. pro $x = -10$ by mělo platit $|-10 \cdot e| = -10$. To ovšem nelze, proto $(G, *)$ nemá neutrální prvek, a tudíž není ani strukturou s inverzními prvky.

Tedy $(G, *)$ není grupa, ale pouze komutativní pologrupa.

b) - Násobení komplexních čísel je asociativní.

- Neutrální prvek:
$(\exists e \in G)\ (\forall x \in G)\ x * e = x$
- označme: $e = k + il\sqrt{5}$
$(a + ib\sqrt{5}) \cdot (k + il\sqrt{5}) = a + ib\sqrt{5}$
$(ak - 5bl) + i\sqrt{5}(al + bk) = a + ib\sqrt{5}$
$(ak - 5bl = a \wedge al + bk = b) \Longrightarrow (k = 1 \wedge l = 0)$
Tedy $e = 1 + i \cdot 0 \cdot \sqrt{5} = 1$ je neutrálním prvkem v $(G, *)$.

- Inverzní prvky:
$(\forall x \in G)\ (\exists \overline{x} \in G)\ x * \overline{x} = e$
- označme: $\overline{x} = p + iq\sqrt{5}$
$(a + ib\sqrt{5}) \cdot (p + iq\sqrt{5}) = 1$
$\overline{x} = p + iq\sqrt{5} = \frac{1}{a + ib\sqrt{5}} = \frac{a - ib\sqrt{5}}{a^2 + 5b^2} = \frac{a}{a^2 + 5b^2} + \frac{-b}{a^2 + 5b^2} \cdot i\sqrt{5} \in G,\ (a^2 + b^2 \neq 0),$
tj. $(G, *)$ je s inverzními prvky.

Tedy $(G, *)$ je komutativní grupa.

Příklad 2. 1. 2:
Napište multiplikativní tabulku grupy $(G, \cdot)$, kde $G = \{e, f, g\}$, když víte, že $e \cdot f = g$.

Řešení:

○	e	f	g
e	f	g	e
f	g	e	f
g	e	f	g

Nejprve doplníme prvek $e \cdot f = g$. Neutrálním prvkem pak může být jedině prvek g, tj. vyplníme třetí řádek a třetí sloupec tabulky. Dále musí být $e \cdot e = f$ (v každém řádku a v každém sloupci tabulky musí být každý prvek právě jednou), potom ze stejného důvodu je $f \cdot e = g$, a nakonec $f \cdot f = e$.

Příklad 2. 1. 3(∗)**:**
Rozhodněte, zda je $(M_2(\mathbb{Z}), +)$ grupa, popřípadě jestli je tato grupa komutativní.

Poznámka:
Symbolem $M_n(T)$ označujeme množinu všech čtvercových matic řádu n nad oborem integrity, resp. polem T.

Řešení:
- Součtem dvou matic z $M_2(\mathbb{Z})$ je opět matice z $M_2(\mathbb{Z})$, tedy $M_2(\mathbb{Z})$ je uzavřená vzhledem k operaci „+“.
- Sčítání matic je asociativní a komutativní, protože je asociativní a komutativní sčítání celých čísel.
- Neutrálním prvkem je nulová matice $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$.
- Ke každému prvku existuje inverzní prvek, k matici $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ je to matice $\begin{pmatrix}-a & -b\\ -c & -d\end{pmatrix}$.

Tedy $(M_2(\mathbb{Z}), +)$ je komutativní grupa.

Příklad 2. 1. 4:
Rozhodněte, zda $(G, \cdot)$ je grupa, kde $G = \{A \in M_n(\mathbb{Z});\ \det A = 1 \vee \det A = -1\}$.

Řešení:
- Součinem dvou čtvercových matic řádu n s celočíselnými prvky je opět čtvercová matice řádu n s celočíselnými prvky.
  Platí: $\det(A \cdot B) = \det A \cdot \det B$
  - je-li $\det A = 1$, $\det B = 1$, pak $\det(A \cdot B) = 1$
  - je-li $\det A = 1$, $\det B = -1$ (nebo naopak), je $\det(A \cdot B) = -1$
  - je-li $\det A = -1$, $\det B = -1$, pak $\det(A \cdot B) = 1$.

  Tedy množina G je uzavřená vzhledem k operaci „$\cdot$“.
- Násobení matic je asociativní, není obecně komutativní.
- Neurálním prvkem je jednotková matice $E = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$.
- Protože $\det A \neq 0$, kde $A \in M_n(\mathbb{Z})$ libovolná, je matice A regulární, proto k ní existuje matice inverzní a platí:
  $A^{-1} = \frac{1}{\det A} \cdot A^*$, kde A^* je adjungovaná matice k matici A (A^* má také celočíselné prvky); $A \cdot A^{-1} = E$, $\det A^{-1} = \frac{1}{\det A}$ (tj. $\det A^{-1} = 1 \vee \det A^{-1} = -1$). To znamená, že $(G, \cdot)$ je strukturou s inverzními prvky.

Tedy $(G, \cdot)$ je (nekomutativní) grupa.

Příklad 2. 1. 5:
Definujme zobrazení $f_i : \mathbb{R} - \{0, 1\} \longrightarrow \mathbb{R} - \{0, 1\}$ pro $i = 1, 2, 3, 4, 5, 6$ takto:
$f_1(x) = x$, $f_2(x) = \frac{1}{x}$, $f_3(x) = 1 - x$, $f_4(x) = \frac{x}{x-1}$, $f_5(x) = \frac{x-1}{x}$, $f_6(x) = \frac{1}{1-x}$.
Dokažte, že pak množina $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ spolu s operací skládání zobrazení je nekomutativní grupa.

Řešení:
Sestavíme Cayleyho tabulku:
Protože skládání zobrazení je asociativní, z tabulky je hned zřejmé, že $(G, \circ)$ je (nekomutativní) grupa.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

Příklad 2. 1. 6:
Nechť $(G, \circ)$ je grupa, $p \in G$ pevný prvek. V množině G definujme operaci „$*$“ takto:
$(\forall\, x, y \in G)\ \ x * y = x \circ p \circ y$.
Rozhodněte, zda $(G, *)$ je grupa.

Řešení:

- Uzavřenost:
  $(\forall\, x, y \in G)\ \ x * y = x \circ p \circ y \in G$ – platí, neboť $(G, \circ)$ je grupa.
- Asociativnost:
  $(\forall\, x, y, z \in G)\ \ (x * y) * z = x * (y * z)$
  $\mathrm{L} = (x * y) * z = (x \circ p \circ y) * z = (x \circ p \circ y) \circ p \circ z = x \circ p \circ y \circ p \circ z$
  $\mathrm{P} = x * (y * z) = x * (y \circ p \circ z) = x \circ p \circ (y \circ p \circ z) = x \circ p \circ y \circ p \circ z$
  Tedy L = P, takže $(G, *)$ je asociativní.
- Neutrální prvek:
  $(\exists\, e \in G)\,(\forall\, x \in G)\ \ x * e = e * x = x$ (neutrální prvek grupy $(G, \circ)$ označme n)

$x * e = x$	$e * x = x$
$x \circ p \circ e = x$	$e \circ p \circ x = x$
$\overline{x} \circ x \circ p \circ e = \overline{x} \circ x$	$e \circ p \circ x \circ \overline{x} = x \circ \overline{x}$ ($\overline{x}$ je inverzní prvek k x v $(G, \circ)$)
$n \circ p \circ e = n$	$e \circ p \circ n = n$
$p \circ e = n$	$e \circ p = n$
$\overline{p} \circ p \circ e = \overline{p} \circ n$	$e \circ p \circ \overline{p} = n \circ \overline{p}$ ($\overline{p}$ je inverzní prvek k p v $(G, \circ)$)
$n \circ e = \overline{p}$	$e \circ n = \overline{p}$
$e = \overline{p}$	$e = \overline{p}$

  Tedy neutrálním prvkem v $(G, *)$ je $\overline{p}$.
- Inverzní prvky:
  $(\forall\, x \in G)\,(\exists\, y \in G)\ \ x * y = y * x = e$

$x * y = \overline{p}$	$y * x = \overline{p}$
$x \circ p \circ y = \overline{p}$	$y \circ p \circ x = \overline{p}$
$\overline{x} \circ x \circ p \circ y = \overline{x} \circ \overline{p}$	$y \circ p \circ x \circ \overline{x} = \overline{p} \circ \overline{x}$
$n \circ p \circ y = \overline{x} \circ \overline{p}$	$y \circ p \circ n = \overline{p} \circ \overline{x}$
$p \circ y = \overline{x} \circ \overline{p}$	$y \circ p = \overline{p} \circ \overline{x}$
$\overline{p} \circ p \circ y = \overline{p} \circ \overline{x} \circ \overline{p}$	$y \circ p \circ \overline{p} = \overline{p} \circ \overline{x} \circ \overline{p}$
$n \circ y = \overline{p} \circ \overline{x} \circ \overline{p}$	$y \circ n = \overline{p} \circ \overline{x} \circ \overline{p}$
$y = \overline{p} \circ \overline{x} \circ \overline{p}$	$y = \overline{p} \circ \overline{x} \circ \overline{p}$

  Tedy $(G, *)$ je strukturou s inverzními prvky.

Struktura $(G, *)$ je grupa.

Příklad 2. 1. 7:
V grupě $(\mathbb{R}^*, \cdot)$ nalezněte všechny prvky konečného řádu a určete jejich řád.

Řešení:
Řád prvku v grupě – viz definice 2. 3.
Číslo 1 je jednotkový prvek grupy $(\mathbb{R}^*, \cdot)$, $o(1) = 1$. Dále $o(-1) = 2$, neboť $(-1)^2 = 1$; ostatní čísla jsou nekonečného řádu, neboť žádná jejich mocnina $n \in \mathbb{Z}^+$ není rovna 1.

Příklad 2. 1. 8:
Zjistěte, zda $(H, \circ)$ je podgrupou grupy $(G, \circ)$, jestliže:

a) $H = \mathbb{Z}_2$, $(G, \circ) = (\mathbb{Z}_4, \oplus)$;
b) $H = \mathbb{Z}_3 - \{\overline{0}\}$, $(G, \circ) = (\mathbb{Z}_4, \oplus)$;

c) $H = \{1, -1\}$, $(G, \circ) = (\mathbb{R}, +)$;
d) $H = \{1, -1\}$, $(G, \circ) = (\mathbb{R}^*, \cdot)$.

Řešení:

a) $(\mathbb{Z}_2, \oplus)$ není podgrupou grupy $(\mathbb{Z}_4, \oplus)$, protože $\mathbb{Z}_2$ není podmnožinou množiny $\mathbb{Z}_4$.

b) Množina $\mathbb{Z}_3 - \{\overline{0}\} = \{\overline{1}, \overline{2}\}$ není uzavřená vzhledem k operaci „$\oplus$“ ($\overline{1} \oplus \overline{2} = \overline{0}$), tedy $(\mathbb{Z}_3 - \{\overline{0}\}, \oplus)$ není ani algebraickou strukturou.

c) Stejný případ jako b), neboť množina $\{1, -1\}$ není uzavřená vzhledem k operaci „+“ (např. $1 + 1 = 2$).

d) Cayleyho tabulka:

$\cdot$	1	–1
1	1	–1
–1	–1	1

- $\{1, -1\}$ je podmnožinou množiny $\mathbb{R}^*$.
- $(\{1, -1\}, \cdot)$ je asociativní (dědičná vlastnost).
- Z Cayleyho tabulky je pak zřejmé, že $(\{1, -1\}, \cdot)$ je grupa.

Příklad 2. 1. 9:

a) Zjistěte, zda $(H, \cdot)$ je podgrupou grupy $(\mathbb{K}^*, \cdot)$, jestliže $H = \{x \in \mathbb{K}; x^n = 1, n \in \mathbb{Z}^+\}$.
b) Nechť $(G, \cdot)$ je komutativní grupa, nechť $H = \{x \in G; x^2 = 1\}$. Dokažte, že $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$.
c) Je dána grupa $(\mathbb{Q}, +)$. Rozhodněte, zda $(H, +)$ je podgrupou grupy $(\mathbb{Q}, +)$, je-li $H = \{\frac{a}{2^k} \in \mathbb{Q}; a, k \in \mathbb{Z}, k \geq 0\}$.

Řešení:

a) - Uzavřenost:
$(\forall x, y \in H)\ x \cdot y \in H$
Jsou-li $x, y \in H$ libovolné, pak $x^n = 1$, $y^n = 1$, a tedy $(x \cdot y)^n = x^n \cdot y^n = 1 \cdot 1 = 1$. To znamená, že $x \cdot y \in H$, neboli množina H je uzavřená vzhledem k operaci „$\cdot$“.

- Asociativnost, komutativnost – platí (dědičné vlastnosti).

- Neutrální prvek:
Protože 1 je neutrálním prvkem $(\mathbb{K}^*, \cdot)$, stačí ověřit, zda $1 \in H$:
$1^n = 1$, tedy 1 je neutrálním prvkem také v $(H, \cdot)$.

- Inverzní prvky:
$(\forall x \in H)\ (\exists x^{-1} \in H)\ x \cdot x^{-1} = 1$
Je-li $x \in H$, pak $x \in \mathbb{K}^*$, a tedy existuje $x^{-1} \in \mathbb{K}^*$; $(x^{-1})^n = x^{-n} = (x^n)^{-1} = 1^{-1} = 1$, takže $x^{-1} \in H$.

Tedy $(H, \cdot)$ je grupa, a protože $H \subseteq \mathbb{K}^*$, je to podgrupa grupy $(\mathbb{K}^*, \cdot)$.

b) - $H \subseteq G$, $H \neq \emptyset$ ($1^2 = 1 \in H$).
- $(\forall x, y \in H)\ x \cdot y^{-1} \in H$
Jsou-li $x, y \in H$ libovolné, pak $x^2 = 1$, $y^2 = 1$; $(x \cdot y^{-1})^2 = x^2 \cdot (y^{-1})^2 = x^2 \cdot (y^2)^{-1} = 1 \cdot 1^{-1} = 1$, tj. $x \cdot y^{-1} \in H$.

Tedy $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$.

c) - $H \subseteq \mathbb{Q}$, $H \neq \emptyset$ ($0 \in H$).
Nechť $x, y \in H$ libovolné. Potom $x = \frac{a}{2^k}$, $y = \frac{b}{2^l}$; $a, b, k, l \in \mathbb{Z}$, $k, l \geq 0$. Bez újmy na obecnosti lze předpokládat, že $k \geq l$. Pak $x - y = \frac{a}{2^k} - \frac{b}{2^l} = \frac{a - b \cdot 2^{k-l}}{2^k} = \frac{c}{2^k}$, $c \in \mathbb{Z}$, tudíž $x - y \in H$.

Tedy $(H, +)$ je podgrupou grupy $(\mathbb{Q}, +)$.

Poznámka:

- Příklad a) jsme řešili použitím definice 2. 1. a při řešení příkladů b), c) jsme zase využili větu 2. 4.;
- v příkladu b) jsme využili §2 na str. 21 a toho, že struktura $(G, \cdot)$ je komutativní.

Příklad 2. 1. 10$(*)$**:**

Nechť $X = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R});\ a \neq 0\}$.

a) Ukažte, že $(X, \cdot)$ je grupa.

b) Zjistěte, zda $(Y, \cdot)$ je podgrupa $(X, \cdot)$, jestliže $Y = \{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R});\ a \neq 0\}$.

Řešení:

a) - Uzavřenost:

Nechť $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in X$ libovolné. Pak

$A \cdot B = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ax & ay + b \\ 0 & 1 \end{pmatrix}$, kde $ax \neq 0$ ($a \neq 0 \wedge x \neq 0$), proto $A \cdot B \in X$.

- Násobení matic je asociativní.

- Neutrálním prvkem je jednotková matice $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in X$.

- Inverzní prvky:

Protože $\det A = a \neq 0$, matice jsou regulární a existuje k nim matice inverzní:

$A^{-1} = \frac{1}{\det A} \cdot A^*$.

$(A^*)^T = \begin{pmatrix} 1 & 0 \\ -b & a \end{pmatrix}$, tedy $A^* = \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix}$, $A^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}$, $\frac{1}{a} \neq 0$, takže $A^{-1} \in X$.

Tedy $(X, \cdot)$ je grupa.

b) - $Y \subseteq X$, $Y \neq \emptyset$ ($E \in Y$).

- $(\forall\, A, B \in Y)\ A \cdot B^{-1} \in Y$

Nechť $A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \in Y$ libovolné. Potom

$A \cdot B^{-1} = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{x} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{a}{x} & 0 \\ 0 & 1 \end{pmatrix} \in Y$ ($a \neq 0$, $x \neq 0$, proto také $\frac{a}{x} \neq 0$).

Tedy $(Y, \cdot)$ je podgrupa grupy $(X, \cdot)$.

Příklad 2. 1. 11:

V grupě $(G, \cdot)$, kde $G = \{A \in M_2(\mathbb{R});\ \det A \neq 0\}$, určete řád matice $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Řešení:

Hledáme $n \in \mathbb{Z}^+$ nejmenší takové, že $A^n = E$:

$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $A^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$,

$A^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $A^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$.

Tedy $o(A) = 4$.

Příklad 2. 1. 12:

Nalezněte všechny podgrupy grupy $(\mathbb{Z}_2 \times \mathbb{Z}_4, \oplus)$ a určete řády všech jejích prvků.

Řešení:

$\mathbb{Z}_2 \times \mathbb{Z}_4 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{0}, \overline{3}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2}), (\overline{1}, \overline{3})\}$.

Sestavíme Cayleyho tabulku pro grupu $(\mathbb{Z}_2 \times \mathbb{Z}_4, \oplus)$, ze které určíme její podgrupy.

$\oplus$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{3})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{1},\overline{3})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{3})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{1},\overline{3})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{3})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{1},\overline{3})$	$(\overline{1},\overline{0})$
$(\overline{0},\overline{2})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{3})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{1},\overline{3})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{3})$	$(\overline{0},\overline{3})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{3})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{2})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{1},\overline{3})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{3})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{1},\overline{3})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{3})$	$(\overline{0},\overline{0})$
$(\overline{1},\overline{2})$	$(\overline{1},\overline{2})$	$(\overline{1},\overline{3})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{0},\overline{3})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{3})$	$(\overline{1},\overline{3})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{3})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{2})$

- Podgrupy:
  Podle Lagrangeovy věty může mít grupa $(\mathbb{Z}_2 \times \mathbb{Z}_4, \oplus)$ pouze podgrupy řádu 1, 2, 4 nebo 8, tedy:
  $(H_1, \oplus) = (\{(\overline{0}, \overline{0})\}, \oplus)$, $(H_2, \oplus) = (\{(\overline{0}, \overline{0}), (\overline{0}, \overline{2})\}, \oplus)$, $(H_3, \oplus) = (\{(\overline{0}, \overline{0}), (\overline{1}, \overline{0}), \oplus)$, $(H_4, \oplus) = (\{(\overline{0}, \overline{0}), (\overline{1}, \overline{2})\}, \oplus)$, $(H_5, \oplus) = (\{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{0}, \overline{3}), \oplus)$, $(H_6, \oplus) = = (\mathbb{Z}_2 \times \mathbb{Z}_4, \oplus)$.
- Řády prvků:
  Hledáme $n \in \mathbb{Z}^+$ nejmenší takové, že $n \times (\overline{a}, \overline{b}) = (\overline{0}, \overline{0})$, kde $(\overline{a}, \overline{b}) \in \mathbb{Z}_2 \times \mathbb{Z}_4$:
  - $(\overline{0}, \overline{0})$…řád 1;
  - $(\overline{0}, \overline{2})$, $(\overline{1}, \overline{0})$, $(\overline{1}, \overline{2})$…řád 2;
  - $(\overline{0}, \overline{1})$, $(\overline{0}, \overline{3})$, $(\overline{1}, \overline{1})$, $(\overline{1}, \overline{3})$…řád 4.

Příklad 2. 1. 13:

V grupě $(\mathbb{Z}_8, \oplus) \times (\mathbb{Z}_8, \oplus)$ určete podgrupu $([M], \oplus)$ generovanou množinou:

$M = \{(\overline{2}, \overline{4}), (\overline{6}, \overline{4})\}$

Řešení:

Podgrupa $([M], \oplus)$ musí obsahovat neutrální prvek grupy $(\mathbb{Z}_8, \oplus) \times (\mathbb{Z}_8, \oplus)$, tj. prvek $(\overline{0}, \overline{0})$. Dále přidáváme postupně prvky z množiny $\mathbb{Z}_8 \times \mathbb{Z}_8$ tak, abychom obdrželi grupu (viz věta 2. 7.):

- $(\overline{2}, \overline{4}) \oplus (\overline{2}, \overline{4}) = (\overline{4}, \overline{0})$
- $(\overline{6}, \overline{4}) \oplus (\overline{6}, \overline{4}) = (\overline{4}, \overline{0})$
- $(\overline{2}, \overline{4}) \oplus (\overline{6}, \overline{4}) = (\overline{0}, \overline{0})$, tj. prvky $(\overline{2}, \overline{4})$, $(\overline{6}, \overline{4})$ jsou navzájem inverzní
- $(\overline{4}, \overline{0}) \oplus (\overline{4}, \overline{0}) = (\overline{0}, \overline{0})$, tj. prvek $(\overline{4}, \overline{0})$ je sám k sobě inverzní
- $(\overline{4}, \overline{0}) \oplus (\overline{2}, \overline{4}) = (\overline{6}, \overline{4})$

- $(\overline{4}, \overline{0}) \oplus (\overline{6}, \overline{4}) = (\overline{2}, \overline{4})$.

Protože struktura $(\mathbb{Z}_8, \oplus) \times (\mathbb{Z}_8, \oplus)$ je komutativní, stačí uvažovat pouze tyto možnosti. Tedy $([M], \oplus) = (\{(\overline{0}, \overline{0}), (\overline{4}, \overline{0}), (\overline{2}, \overline{4}), (\overline{6}, \overline{4})\}, \oplus) = ([(\overline{2}, \overline{4})], \oplus) = ([(\overline{6}, \overline{4})], \oplus)$.

Příklad 2. 1. 14:
V množině $G = \{1, 2, 3, \ldots, 12\}$ je definovaná operace „$\oplus$“ takto:
$x \oplus y = x + y$, pro $x + y \leq 12$;
$x \oplus y = x + y - 12$, pro $x + y > 12$.

Dokažte, že $(G, \oplus)$ je komutativní grupa. Vypište všechny její podgrupy a nakreslete Hasseův diagram uspořádané množiny $(\mathscr{S}, \subseteq)$, kde $\mathscr{S}$ značí množinu všech podgrup grupy $(G, \oplus)$. Dále nalezněte v grupě $(G, \oplus)$ podgrupu $([M], \oplus)$, jestliže:
a) $M = \{3, 6\}$ b) $M = \{4\}$ c) $M = \{1\}$.

Řešení:

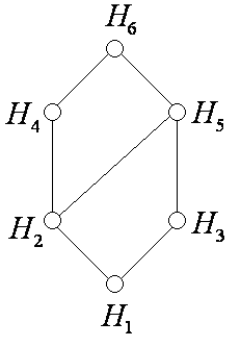
- Sestavíme Cayleyho tabulku:

$\oplus$	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
4	5	6	7	8	9	10	11	12	1	2	3	4
5	6	7	8	9	10	11	12	1	2	3	4	5
6	7	8	9	10	11	12	1	2	3	4	5	6
7	8	9	10	11	12	1	2	3	4	5	6	7
8	9	10	11	12	1	2	3	4	5	6	7	8
9	10	11	12	1	2	3	4	5	6	7	8	9
10	11	12	1	2	3	4	5	6	7	8	9	10
11	12	1	2	3	4	5	6	7	8	9	10	11
12	1	2	3	4	5	6	7	8	9	10	11	12

  Protože operace „$\oplus$“ je asociativní, z Cayleyho tabulky je zřejmé, že $(G, \oplus)$ je komutativní grupa.

- Podgrupy:
  $(H_1, \oplus) = (\{12\}, \oplus)$, $(H_2, \oplus) = (\{12, 6\}, \oplus)$, $(H_3, \oplus) = (\{12, 4, 8\}, \oplus)$, $(H_4, \oplus) = (\{12, 3, 6, 9\}, \oplus)$, $(H_5, \oplus) = (\{12, 2, 4, 6, 8, 10\}, \oplus)$, $(H_6, \oplus) = (G, \oplus)$.

- Hasseův diagram:



- Při hledání $([M], \oplus)$ využíváme definici 2. 4.:
  a) $([M], \oplus) = ([3, 6], \oplus) = (H_4, \oplus)$,
  b) $([M], \oplus) = ([4], \oplus) = (H_3, \oplus)$,
  c) $([M], \oplus) = ([1], \oplus) = (H_6, \oplus)$.

3. 2. 2. Příklady k procvičení

Příklad 2. 2. 1:
Je dán komutativní grupoid $(G, *)$. Rozhodněte, zda $(G, *)$ je komutativní grupou, jestliže:
a) $G = \mathbb{Q}^+$, operace „$*$“ je násobení racionálních čísel.
b) $G = \{a + bi; a, b \in \mathbb{Z}\}$, operace „$*$“ je sčítání komplexních čísel.

Příklad 2. 2. 2:
Nechť A je libovolná pevná množina. Dokažte, že potom $(P(A), \div)$ je komutativní grupa.

Příklad 2. 2. 3:
Rozhodněte, zda je daná struktura grupa.
a) $(M_n(\mathbb{K}), +)$;
b) $(M_n(\mathbb{R}), \cdot)$;
c) $(G, \cdot)$, kde $G = \{A \in M_n(\mathbb{Q}); \det A \neq 0\}$.

Příklad 2. 2. 4:
Zjistěte, zda $(H, \circ)$ je podgrupou grupy $(G, \circ)$, jestliže:
a) $H = \mathbb{N}$, $(G, \circ) = (\mathbb{Z}, +)$;
b) $H = \mathbb{Q}^+$, $(G, \circ) = (\mathbb{Q}, +)$;
c) $H = \mathbb{Q}^+$, $(G, \circ) = (\mathbb{Q} - \{0\}, \cdot)$.

Příklad 2. 2. 5:
Zjistěte, zda $(H, \cdot)$ je podgrupou grupy $(\mathbb{K}^*, \cdot)$, jestliže:
a) $H = \{x \in \mathbb{K}; |x| = 1\}$;
b) $H = \{x \in \mathbb{K}^*; x$ je reálné číslo nebo x je ryze imaginární číslo$\}$.

Příklad 2. 2. 6:
Nechť $(G, \cdot)$ je komutativní grupa, nechť $H = \{a \in G; (\exists\, n \in \mathbb{Z}^+)\ a^n = 1\}$. Dokažte, že $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$.

Příklad 2. 2. 7:
Určete řády všech prvků v grupě $(G, \circ)$, jestliže:
a) $G = P(M)$, $M = \{1, 2\}$, $A \circ B = A \div B$, $A, B \in P(M)$;
b) $(G, \circ) = (\mathbb{Z}_8, \oplus)$.

3. 3. Cyklické grupy

3. 3. 1. Řešené příklady

Příklad 3. 1. 1:
Nalezněte všechny generátory grupy:

a) $(\mathbb{Z}_6, \oplus)$;
b) $(\mathbb{Z}_{13}, \oplus)$;
c) $(\mathbb{Z}_{18}, \oplus)$.

Řešení:
Pro každé $m \in \mathbb{Z}$, $m > 1$: $(\mathbb{Z}_m, \oplus) = [\overline{1}] = [k \times \overline{1}] = [\overline{k}]$, právě když $nsd(k, m) = 1$ (využíváme větu 3. 11.)

a) $nsd(k, 6) = 1 \Leftrightarrow k = 1, 5$
$(\mathbb{Z}_6, \oplus) = [\overline{1}] = [\overline{5}]$.
b) $nsd(k, 13) = 1 \Leftrightarrow k = 1, 2, 3, 4, \ldots, 12$
$(\mathbb{Z}_{13}, \oplus) = [\overline{1}] = [\overline{2}] = [\overline{3}] = [\overline{4}] = \ldots = [\overline{12}]$.
c) $nsd(k, 18) = 1 \Leftrightarrow k = 1, 5, 7, 11, 13, 17$
$(\mathbb{Z}_{18}, \oplus) = [\overline{1}] = [\overline{5}] = [\overline{7}] = [\overline{11}] = [\overline{13}] = [\overline{17}]$.

Příklad 3. 1. 2:
Jsou dány grupy:

a) $G = (\{x \in \mathbb{Q}; x = 3^k, k \in \mathbb{Z}\}, \cdot)$;
b) $G = (\{x \in \mathbb{Q}; x = \frac{1}{2^k}, k \in \mathbb{Z}\}, \cdot)$.

Určete všechny generátory těchto grup.

Řešení:

a) $G = [3] = [\frac{1}{3}]$.
b) $G = [\frac{1}{2}] = [2]$.

Poznámka:
Využíváme větu 3. 3., větu 3. 4.

Příklad 3. 1. 3:
V grupách $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$ určete podgrupu H generovanou prvkem $\sqrt[5]{3}$.

Řešení:

- $(\mathbb{R}, +)$: $H = [\sqrt[5]{3}] = (\{x \in \mathbb{R}; x = k \cdot \sqrt[5]{3}, k \in \mathbb{Z}\}, +)$;
- $(\mathbb{R}^*, \cdot)$: $H = [\sqrt[5]{3}] = (\{x \in \mathbb{R}^*; x = (\sqrt[5]{3})^k, k \in \mathbb{Z}\}, \cdot)$.

Příklad 3. 1. 4:
Určete počet generátorů cyklické grupy G řádu:

a) 24 b) 81.

Řešení:
Využijeme Eulerovu funkci φ (viz poznámka 2) str. 27); dále využijeme toho, že platí:

- pro $m, n \in \mathbb{Z}^+$, $nsd(m, n) = 1$, je $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

a) $G \cong (\mathbb{Z}_{24}, \oplus)$, $24 = 2^3 \cdot 3$, $\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3) \cdot \varphi(3) = (2^3 - 2^2) \cdot (3 - 1) = 8$.
Tedy grupa G má 8 generátorů.

b) $G \cong (\mathbb{Z}_{81}, \oplus)$, $81 = 3^4$, $\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 54$, tj. grupa G má 54 generátorů.

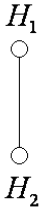
Příklad 3. 1. 5:
V dané grupě $(\mathbb{Z}_m, \oplus)$ vypište všechny její podgrupy a nakreslete Hasseův diagram uspořádané množiny $(\mathscr{S}, \subseteq)$, kde $\mathscr{S}$ značí množinu všech podgrup grupy $(\mathbb{Z}_m, \oplus)$. Přitom daná grupa je:

a) $(\mathbb{Z}_3, \oplus)$ b) $(\mathbb{Z}_{12}, \oplus)$ c) $(\mathbb{Z}_{21}, \oplus)$.

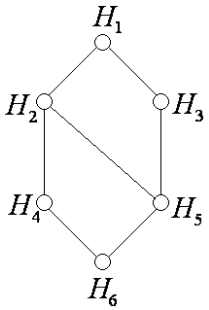
Řešení:

Všechny podgrupy grupy $(\mathbb{Z}_m, \oplus)$ jsou tvořeny množinou $\{[d \times \overline{1}]; d \in \mathbb{Z}^+, d \mid m\}$.

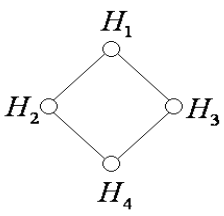
a) $m = 3$: $d \mid 3 \Leftrightarrow d = 1, 3$
Podgrupy:
$H_1 = [1 \times \overline{1}] = [\overline{1}] = (\mathbb{Z}_3, \oplus)$, $H_2 = [3 \times \overline{1}] = [\overline{0}] = (\{\overline{0}\}, \oplus)$.
Hasseův diagram:



b) $m = 12$: $d \mid 12 \Leftrightarrow d = 1, 2, 3, 4, 6, 12$
Podgrupy:
$H_1 = [1 \times \overline{1}] = [\overline{1}] = (\mathbb{Z}_{12}, \oplus)$, $H_2 = [2 \times \overline{1}] = [\overline{2}] = (\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}, \oplus)$,
$H_3 = [3 \times \overline{1}] = [\overline{3}] = (\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}, \oplus)$, $H_4 = [4 \times \overline{1}] = [\overline{4}] = (\{\overline{0}, \overline{4}, \overline{8}\}, \oplus)$,
$H_5 = [6 \times \overline{1}] = [\overline{6}] = (\{\overline{0}, \overline{6}\}, \oplus)$, $H_6 = [12 \times \overline{1}] = [\overline{0}] = (\{\overline{0}\}, \oplus)$.
Hasseův diagram:



c) $m = 21$: $d \mid 21 \Leftrightarrow d = 1, 3, 7, 21$
Podgrupy:
$H_1 = [1 \times \overline{1}] = [\overline{1}] = (\mathbb{Z}_{21}, \oplus)$, $H_2 = [3 \times \overline{1}] = [\overline{3}] = (\{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}, \overline{18}\}, \oplus)$,
$H_3 = [7 \times \overline{1}] = [\overline{7}] = (\{\overline{0}, \overline{7}, \overline{14}\}, \oplus)$, $H_4 = [21 \times \overline{1}] = [\overline{0}] = (\{\overline{0}\}, \oplus)$.
Hasseův diagram:



Poznámka: Využíváme větu 3. 12.

Příklad 3. 1. 6:
V grupě $(\mathbb{Z}_{16}, \oplus)$ nalezněte podgrupu $[M]$, jestliže:

a) $M = \emptyset$ b) $M = \{\overline{3}\}$ c) $M = \{\overline{6}\}$ d) $M = \{\overline{4}, \overline{8}\}$.

Řešení:
$m = 16$: $d \mid 16 \Leftrightarrow d = 1, 2, 4, 8, 16$
Podgrupy:
$H_1 = [\overline{1}] = (\mathbb{Z}_{16}, \oplus)$, $H_2 = [\overline{2}] = (\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}\}, \oplus)$, $H_3 = [\overline{4}] = (\{\overline{0}, \overline{4}, \overline{8}, \overline{12}\}, \oplus)$, $H_4 = [\overline{8}] = (\{\overline{0}, \overline{8}\}, \oplus)$, $H_5 = (\{\overline{0}\}, \oplus)$.

a) $[M] = [\emptyset] = H_5$,
b) $[M] = [\overline{3}] = H_1$,
c) $[M] = [\overline{6}] = H_2$,
d) $[M] = [\overline{4}, \overline{8}] = H_3$.

Příklad 3. 1. 7:
Je dána množina komplexních čísel $M = \{1, -1, i, -i\}$. Ověřte, že struktura $(M, \cdot)$, kde operace „$\cdot$“ je násobení komplexních čísel, je grupa. Dále určete podgrupy $[A]$, jestliže:

a) $A = \{1\}$ b) $A = \{-1\}$ c) $A = \{i\}$ d) $A = \{-i\}$.

Řešení:

- Sestavíme Cayleyho tabulku:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

  - Protože násobení komplexních čísel je asociativní, z tabulky je zřejmé, že $(M, \cdot)$ je grupa.

- a) $[A] = [1] = (\{1\}, \cdot)$,
  b) $[A] = [-1] = (\{1, -1\}, \cdot)$,
  c), d) $[A] = [i] = [-i] = (M, \cdot)$.

Příklad 3. 1. 8:
V grupě $(\mathbb{K}^*, \cdot)$ určete podgrupu A generovanou prvkem $a = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$.
Řešení:
Řád prvku v grupě je řád cyklické podgrupy generované daným prvkem. Určíme tedy řád prvku a:

- $a = \frac{1}{2}(\sqrt{2} + i\sqrt{2})$, $a^2 = i$, $a^3 = \frac{1}{2}(-\sqrt{2} + i\sqrt{2})$, $a^4 = -1$, $a^5 = \frac{1}{2}(-\sqrt{2} - i\sqrt{2})$, $a^6 = -i$, $a^7 = \frac{1}{2}(\sqrt{2} - i\sqrt{2})$, $a^8 = 1$.

Tedy $A = [a] = (\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = 1\}, \cdot)$.

Příklad 3. 1. 9($*$):
Dokažte, že grupa všech řešení rovnice $x^3 - 1 = 0$ spolu s operací násobení komplexních čísel je podgrupou grupy všech řešení rovnice $x^6 - 1 = 0$. Určete řády všech prvků těchto grup. Jsou to cyklické grupy? Jestliže ano, najděte všechny generátory obou grup.

Řešení:
Označme: $A = (\{x \in \mathbb{K}; x^3 - 1 = 0\}, \cdot)$, $B = (\{x \in \mathbb{K}; x^6 - 1 = 0\}, \cdot)$.

Kořeny rovnice $x^3 - 1 = 0$: $x_1 = 1$, $x_2 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $x_3 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$.

Kořeny rovnice $x^6 - 1 = 0$: $x_1 = 1$, $x_2 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $x_3 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, $x_4 = -1$, $x_5 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, $x_6 = \frac{1}{2} - i\frac{\sqrt{3}}{2}$.

Cayleyho tabulka pro $(B, \cdot)$:

$\cdot$	x_1	x_2	x_3	x_4	x_5	x_6
x_1	x_1	x_2	x_3	x_4	x_5	x_6
x_2	x_2	x_3	x_1	x_6	x_4	x_5
x_3	x_3	x_1	x_2	x_5	x_6	x_4
x_4	x_4	x_6	x_5	x_1	x_3	x_2
x_5	x_5	x_4	x_6	x_3	x_2	x_1
x_6	x_6	x_5	x_4	x_2	x_1	x_3

- Z tabulky je zřejmé, že $(A, \cdot)$ je podgrupou (řádu 3) grupy $(B, \cdot)$, která je řádu 6.

Řády prvků:
- $o(x_1) = 1$ (x_1 je neutrální prvek),
- $o(x_4) = 2$ ($x_4^2 = x_1$),
- $o(x_2) = o(x_3) = 3$ ($x_2^2 = x_3$, $x_2^3 = x_1$; $x_3^2 = x_2$, $x_3^3 = x_1$),
- $o(x_5) = o(x_6) = 6$ ($x_5^2 = x_2$, $x_5^3 = x_4$, $x_5^4 = x_3$, $x_5^5 = x_6$, $x_5^6 = x_1$; $x_6^2 = x_3$, $x_6^3 = x_4$, $x_6^4 = x_2$, $x_6^5 = x_5$, $x_6^6 = x_1$).

Na základě řádů prvků pak dostáváme:
- $A = [x_2] = [x_3]$,
- $B = [x_5] = [x_6]$.

Příklad 3. 1. 10:
Nechť $\varphi: \mathbb{K} \longrightarrow \mathbb{K}$, $\psi: \mathbb{K} \longrightarrow \mathbb{K}$ jsou zobrazení definované předpisem:
$(\forall\, x \in \mathbb{K})\ \ \varphi(x) = 4x,\ \ \psi(x) = 2 - 4x$.
Označme:
$f_1(x) = \frac{\varphi(x)}{4}$, $f_2(x) = \frac{1}{2} - \frac{1}{\psi(x)}$, $f_3(x) = \frac{1}{\varphi(x)}$, $f_4(x) = \frac{\psi(x)}{4}$, $f_5(x) = \frac{1}{2} - \frac{1}{\varphi(x)}$, $f_6(x) = \frac{1}{\psi(x)}$.
Ověřte, že $A = (\{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ)$, kde operace „$\circ$“ je skládání zobrazení, je grupa, nalezněte všechny její podgrupy a nakreslete pro ně Hasseův diagram. Dále zjistěte, zda grupa A a její podgrupy jsou cyklické. Pokud ano, najděte všechny jejich generátory.

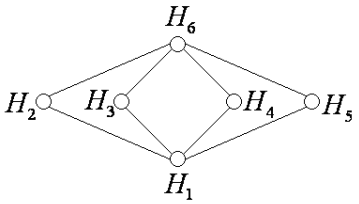
Řešení:

- Sestavíme Cayleyho tabulku (stejná jako v příkladě 2. 1. 5), z níž je zřejmé, že A je grupa.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

- Podgrupy:
  $H_1 = (\{f_1\}, \circ)$, $H_2 = (\{f_1, f_2\}, \circ)$, $H_3 = (\{f_1, f_3\}, \circ)$, $H_4 = (\{f_1, f_4\}, \circ)$, $H_5 = (\{f_1, f_5, f_6\}, \circ)$, $H_6 = A$.

- Hasseův diagram:



- Zda grupa A a její podgrupy jsou cyklické, zjistíme tak, že určíme řády všech prvků grupy A:
  - $o(f_1) = 1$ (f_1 je neutrální prvek),
  - $o(f_2) = o(f_3) = o(f_4) = 2$ ($f_i^{\circ 2} = f_1$, $i = 2, 3, 4$),
  - $o(f_5) = o(f_6) = 3$ ($f_i^{\circ 3} = f_1$, $i = 5, 6$).

  Tedy máme:
  - $H_1 = [f_1]$, $H_2 = [f_2]$, $H_3 = [f_3]$, $H_4 = [f_4]$, $H_5 = [f_5] = [f_6]$.
  - Protože žádný prvek grupy A není řádu 6, grupa A není cyklická.

Poznámka:
Dá se dokázat, že platí:
Je-li p prvočíslo, pak $(\mathbb{Z}_p^*, \odot) \cong (\mathbb{Z}_{p-1}, \oplus)$, a tedy $(\mathbb{Z}_p^*, \odot)$ je cyklická grupa.

Příklad 3. 1. 11:
Určete všechny generátory a všechny podgrupy grupy $(\mathbb{Z}_5^*, \odot)$ a $(\mathbb{Z}_7^*, \odot)$.
Řešení:

- $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$
  Platí: $(\mathbb{Z}_p^*, \odot) = [\ \overline{a}\ ] = [\ \overline{a}^{\,k}\ ] \Leftrightarrow nsd(k, |\mathbb{Z}_p^*|) = 1$, $\overline{a} \in \mathbb{Z}_p^*$.
  Protože $\overline{1}$ je neutrální prvek, nemůže být generátorem grupy $(\mathbb{Z}_5^*, \odot)$, která je řádu 4.
  Zkusme prvek $\overline{2}$:
  - $\overline{2}^1 = \overline{2}$, $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{3}$, $\overline{2}^4 = \overline{1}$, tedy $(\mathbb{Z}_5^*, \odot) = [\overline{2}]$,
  - $nsd(k, 4) = 1 \Leftrightarrow k = 1, 3$; proto také $(\mathbb{Z}_5^*, \odot) = [\overline{2}^3] = [\overline{3}]$.

  Podgrupy:
  - tvořeny množinou $\{[\overline{a}^{\,d}]; d \in \mathbb{Z}^+, d \text{ dělí } |\mathbb{Z}_p^*|\}$,
  - $|\mathbb{Z}_p^*| = 4$: $d \mid 4 \Leftrightarrow d = 1, 2, 4$
    $H_1 = [\overline{2}^1] = [\overline{2}] = (\mathbb{Z}_5^*, \odot)$, $H_2 = [\overline{2}^2] = [\overline{4}] = (\{\overline{1},\overline{4}\}, \odot)$, $H_3 = [\overline{2}^4] = [\overline{1}] = (\{\overline{1}\}, \odot)$.

- $\mathbb{Z}_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$
  - $\overline{3}^1 = \overline{3}$, $\overline{3}^2 = \overline{2}$, $\overline{3}^3 = \overline{6}$, $\overline{3}^4 = \overline{4}$, $\overline{3}^5 = \overline{5}$, $\overline{3}^6 = \overline{1}$, tedy $(\mathbb{Z}_7^*, \odot) = [\overline{3}]$,
  - $nsd(k, 6) = 1 \Leftrightarrow k = 1, 5$; proto také $(\mathbb{Z}_5^*, \odot) = [\overline{3}^5] = [\overline{5}]$.

  Podgrupy:
  - $|\mathbb{Z}_p^*| = 6$: $d \mid 6 \Leftrightarrow d = 1, 2, 3, 6$
  - $H_1 = [\overline{3}] = (\mathbb{Z}_7^*, \odot)$, $H_2 = [\overline{3}^2] = [\overline{2}] = (\{\overline{1}, \overline{2}, \overline{4}\}, \odot)$, $H_3 = [\overline{3}^3] = [\overline{6}] = (\{\overline{1}, \overline{6}\}, \odot)$, $H_4 = [\overline{3}^6] = [\overline{1}] = (\{\overline{1}\}, \odot)$.

Poznámka:
Obecně je obtížné určit generátor grupy $(\mathbb{Z}_p^*, \odot)$.

Příklad 3. 1. 12(∗)**:**
Dokažte, že $(\mathbb{Z}_6, \oplus) \cong (\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$.

Řešení:
Libovolné $k \in \mathbb{Z}$ lze podle věty o dělení se zbytkem v $\mathbb{Z}$ zapsat ve tvaru: $k = mq + k_m$, kde $0 \leq k_m < m$, $m \in \mathbb{Z}^+$, $q \in \mathbb{Z}$. Pro naše účely: $k = 6q + k_6$, $k = 2q' + k_2$, $k = 3q'' + k_3$.
Definujme zobrazení φ: $(\mathbb{Z}_6, \oplus) \longrightarrow (\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ předpisem:
$(\forall k_6 \in \mathbb{Z}_6)\ \ \varphi(k_6) = (k_2, k_3)$

a) Ukážeme, že φ je bijekce.
   - Nechť $k, l \in \mathbb{Z}$ libovolné takové, že $k_6 = l_6$. Pak $6 \mid k - l$, tedy $2 \mid k - l$ a zároveň $3 \mid k - l$. Odtud $k_2 = l_2$, $k_3 = l_3$, takže $(k_2, k_3) = (l_2, l_3)$, neboli $\varphi(k_6) = \varphi(l_6)$. To znamená, že φ je zobrazení.
   - φ je zobrazení celé množiny.
   - Nechť $k, l \in \mathbb{Z}$ libovolné takové, že $\varphi(k_6) = \varphi(l_6)$. Potom $(k_2, k_3) = (l_2, l_3)$, takže $k_2 = l_2$ a zároveň $k_3 = l_3$, tedy $2 \mid k - l$ a také $3 \mid k - l$; přitom $nsd(2, 3) = 1$. Odtud dostáváme $6 \mid k - l$, neboli $k_6 = l_6$. To znamená, že φ je injekce.
   - Injektivní zobrazení celé množiny musí být na množinu, tedy φ je surjekce.

   Dohromady φ je bijekce.

b) Ukážeme, že φ je homomorfismus
   Podle definice operace „⊕“ v $\mathbb{Z}_m$ je $k_m \oplus l_m = (k + l)_m$.
   $(\forall k_6, l_6 \in \mathbb{Z}_6)\ \ \varphi(k_6 \oplus l_6) = \varphi((k + l)_6) = ((k + l)_2, (k + l)_3) = (k_2 \oplus l_2, k_3 \oplus l_3) =$
   $= (k_2, k_3) \oplus (l_2, l_3) = \varphi(k_6) \oplus \varphi(l_6)$ – splněna podmínka homomorfismu.

Tedy φ je izomorfismus, tj. $(\mathbb{Z}_6, \oplus) \cong (\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$.

Poznámka:
Právě dokázané tvrzení je speciálním případem tzv. Čínské věty o zbytcích (viz poznámka na straně 26).

Příklad 3. 1. 13:
Jsou dány grupy: $(\mathbb{Z}_3 \times \mathbb{Z}_4, \oplus)$, $(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \oplus)$, $(\mathbb{Z}_6 \times \mathbb{Z}_8, \oplus)$.
Zjistěte, zda jsou tyto grupy cyklické. V kladném případě určete jejich generátory.

Řešení:

- Protože $nsd(3, 4) = 1$, tak podle Čínské věty o zbytcích je $(\mathbb{Z}_3 \times \mathbb{Z}_4, \oplus) \cong (\mathbb{Z}_{12}, \oplus)$. Tedy $(\mathbb{Z}_3 \times \mathbb{Z}_4, \oplus)$ je cyklická grupa.
  Generátory určíme dvěma způsoby:
  - $(\mathbb{Z}_{12}, \oplus) = [\overline{1}] = [\overline{5}] = [\overline{7}] = [\overline{11}]$.
    Každému generátoru grupy $(\mathbb{Z}_{12}, \oplus)$ přiřadíme uspořádanou dvojici ze $\mathbb{Z}_3 \times \mathbb{Z}_4$:
    $\overline{1} \leftrightarrow (\overline{1}, \overline{1})$, $\overline{5} \leftrightarrow (\overline{2}, \overline{1})$, $\overline{7} \leftrightarrow (\overline{1}, \overline{3})$, $\overline{11} \leftrightarrow (\overline{2}, \overline{3})$.
    Tedy $(\mathbb{Z}_3 \times \mathbb{Z}_4, \oplus) = [(\overline{1}, \overline{1})] = [(\overline{2}, \overline{1})] = [(\overline{1}, \overline{3})] = [(\overline{2}, \overline{3})]$.
  - Určíme generátory grupy $(\mathbb{Z}_3, \oplus)$ a $(\mathbb{Z}_4, \oplus)$. Z nich potom sestavíme všechny uspořádané dvojice, čímž získáme všechny generátory grupy $(\mathbb{Z}_3 \times \mathbb{Z}_4, \oplus)$.
    $(\mathbb{Z}_3, \oplus) = [\overline{1}] = [\overline{2}]$, $(\mathbb{Z}_4, \oplus) = [\overline{1}] = [\overline{3}]$.
    Tedy $(\mathbb{Z}_3 \times \mathbb{Z}_4, \oplus) = [(\overline{1}, \overline{1})] = [(\overline{1}, \overline{3})] = [(\overline{2}, \overline{1})] = [(\overline{2}, \overline{3})]$.
- Grupa $(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \oplus)$ je cyklická, neboť $nsd(2, 3, 5) = 1$, a tudíž podle Čínské věty o zbytcích je $(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \oplus) \cong (\mathbb{Z}_{30}, \oplus)$.

Generátory:

- $(\mathbb{Z}_{30}, \oplus) = [\overline{1}] = [\overline{7}] = [\overline{11}] = [\overline{13}] = [\overline{17}] = [\overline{19}] = [\overline{23}] = [\overline{29}]$.
  $\overline{1} \leftrightarrow (\overline{1}, \overline{1}, \overline{1})$, $\overline{7} \leftrightarrow (\overline{1}, \overline{1}, \overline{2})$, $\overline{11} \leftrightarrow (\overline{1}, \overline{2}, \overline{1})$, $\overline{13} \leftrightarrow (\overline{1}, \overline{1}, \overline{3})$,
  $\overline{17} \leftrightarrow (\overline{1}, \overline{2}, \overline{2})$, $\overline{19} \leftrightarrow (\overline{1}, \overline{1}, \overline{4})$, $\overline{23} \leftrightarrow (\overline{1}, \overline{2}, \overline{3})$, $\overline{29} \leftrightarrow (\overline{1}, \overline{2}, \overline{4})$.

  $(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \oplus) = [(\overline{1}, \overline{1}, \overline{1})] = [(\overline{1}, \overline{1}, \overline{2})] = [(\overline{1}, \overline{2}, \overline{1})] = [(\overline{1}, \overline{1}, \overline{3})] =$
  $= [(\overline{1}, \overline{2}, \overline{2})] = [(\overline{1}, \overline{1}, \overline{4})] = [(\overline{1}, \overline{2}, \overline{3})] = [(\overline{1}, \overline{2}, \overline{4})]$.
- $(\mathbb{Z}_2, \oplus) = [\overline{1}]$, $(\mathbb{Z}_3, \oplus) = [\overline{1}] = [\overline{2}]$, $(\mathbb{Z}_5, \oplus) = [\overline{1}] = [\overline{2}] = [\overline{3}] = [\overline{4}]$.
  Vytvoříme z generátorů těchto grup všechny uspořádané trojice, což jsou generátory grupy $(\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5, \oplus)$.

- Protože $nsd(6, 8) = 2 > 1$, grupy $(\mathbb{Z}_{48}, \oplus)$ a $(\mathbb{Z}_6 \times \mathbb{Z}_8, \oplus)$ nejsou izomorfní, neboť grupa $(\mathbb{Z}_{48}, \oplus)$ obsahuje prvek $\overline{1}$ řádu 48, ale grupa $(\mathbb{Z}_6 \times \mathbb{Z}_8, \oplus)$ má všechny prvky nejvýše řádu $nsn(6, 8) = 24$.
  Opravdu:
  $(\forall\ (\overline{a}, \overline{b}) \in \mathbb{Z}_6 \times \mathbb{Z}_8)\ \ 24 \times (\overline{a}, \overline{b}) = (24 \times \overline{a}, 24 \times \overline{b}) = (4 \times (6 \times \overline{a}), 3 \times (8 \times \overline{b})) =$
  $= (4 \times \overline{0}, 3 \times \overline{0}) = (\overline{0}, \overline{0})$.

3. 3. 2. Příklady k procvičení

Příklad 3. 2. 1:
Nalezněte všechny generátory grupy:

a) $(\mathbb{Z}_7, \oplus)$;
b) $(\mathbb{Z}_{14}, \oplus)$;
c) $(\mathbb{Z}_{20}, \oplus)$.

Příklad 3. 2. 2:
V dané grupě $(\mathbb{Z}_m, \oplus)$ vypište všechny její podgrupy a nakreslete Hasseův diagram uspořádané množiny $(\mathscr{S}, \subseteq)$, kde $\mathscr{S}$ značí množinu všech podgrup grupy $(\mathbb{Z}_m, \oplus)$. Přitom daná grupa je:

a) $(\mathbb{Z}_5, \oplus)$;
b) $(\mathbb{Z}_{30}, \oplus)$.

Příklad 3. 2. 3:
Určete všechny generátory a všechny podgrupy grupy $(\mathbb{Z}_{11}^*, \odot)$.

Příklad 3. 2. 4:
Nechť $A = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\} \subseteq \mathbb{Z}_8$, $B = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\} \subseteq \mathbb{Z}_9$. Zjistěte, zda množiny A, B jsou spolu s operací „$\odot$“ cyklické grupy. Pokud ano, nalezněte všechny generátory obou grup. Dále určete všechny jejich podgrupy a znázorněte je Hasseovým diagramem.

Příklad 3. 2. 5:
Jsou dány grupy $(\mathbb{Z}_6 \times \mathbb{Z}_7, \oplus)$ a $(\mathbb{Z}_5 \times \mathbb{Z}_{10}, \oplus)$. Zjistěte, zda jsou tyto grupy cyklické. V kladném případě určete jejich generátory.

3. 4. Rozklady podle podgrupy

3. 4. 1. Řešené příklady

Příklad 4. 1. 1(∗)**:**
Určete faktorovou grupu grupy $(\mathbb{Z}, +)$ podle podgrupy $[k]$, kde $k \in \mathbb{N}$.

Řešení:
$\mathbb{Z}/[k] = \{x + [k]\}_{x \in \mathbb{Z}}$

- $k = 0$: $\mathbb{Z}/[0] = \{x + [0]\}_{x \in \mathbb{Z}} = \{x + \{0\}\}_{x \in \mathbb{Z}} = \{\{x\}\}_{x \in \mathbb{Z}}$, tj. $(\mathbb{Z}/[0], +) \cong (\mathbb{Z}, +)$;
- $k = 1$: $\mathbb{Z}/[1] = \{x + [1]\}_{x \in \mathbb{Z}} = \{x + \mathbb{Z}\}_{x \in \mathbb{Z}} = \{\mathbb{Z}\}$, tj. $(\mathbb{Z}/[1], +) \cong (\{0\}, +)$;
- $k \neq 0$, $k \neq 1$, $k \in \mathbb{N}$:
  Určíme třídy rozkladu:
  - $x = 0$: $0 + [k] = \{y \in \mathbb{Z}; y = kq, q \in \mathbb{Z}\} = [k]$,
  - $x = 1$: $1 + [k] = \{y \in \mathbb{Z}; y = 1 + kq, q \in \mathbb{Z}\}$,
    ⋮
  - $x = k - 1$: $(k-1) + [k] = \{y \in \mathbb{Z}; y = (k-1) + kq, q \in \mathbb{Z}\}$.

  $\mathbb{Z}/[k] = \{[k], 1 + [k], \ldots, (k-1) + [k]\}$, tj. $(\mathbb{Z}/[k], +) \cong (\mathbb{Z}_k, \oplus)$.

Příklad 4. 1. 2(∗)**:**
Určete třídy rozkladu grupy G podle podgrupy H, jestliže:

a) $G = (\mathbb{K}^*, \cdot)$, $H = (\{z \in \mathbb{K}; |z| = 1\}, \cdot)$;
b) $G = (\mathbb{K}^*, \cdot)$, $H = (\mathbb{R}^+, \cdot)$;
c) $G = (\mathbb{R}^*, \cdot)$, $H = (\{1, -1\}, \cdot)$;
d) $G = (\mathbb{K}, +)$, $H = (\mathbb{R}, +)$;
e) $G = (\mathbb{R}^*, \cdot)$, $H = (\mathbb{R}^+, \cdot)$.

Řešení:
Stačí hledat např. levé třídy rozkladu, protože všechny uvedené struktury jsou komutativní.
Obecně: $G/H = \{xH\}_{x \in G} = \{xH; x \in G\}$ (multiplikativní zápis);
$G/H = \{x + H\}_{x \in G} = \{x + H; x \in G\}$ (aditivní zápis).

a) $G/H = \mathbb{K}^*/H = \{xH\}_{x \in \mathbb{K}^*}$
   Určíme třídy rozkladu (dvojím způsobem):
   - $xH = \{y \in G; y = xh, h \in H\} = \{y \in \mathbb{K}^*; |y| = |xh|, h \in H\} =$
     $= \{y \in \mathbb{K}^*; |y| = |x| \cdot |h|, h \in H\} = \{y \in \mathbb{K}^*; |y| = |x|\}$;
   - Platí: $xH = yH \Leftrightarrow y^{-1}x \in H \Leftrightarrow x^{-1}y \in H$.
     Tedy: $xH = yH \Leftrightarrow \frac{y}{x} \in H \Leftrightarrow |\frac{y}{x}| = 1 \Leftrightarrow |y| = |x|$.

b) $G/H = \mathbb{K}^*/\mathbb{R}^+ = \{x\mathbb{R}^+\}_{x \in \mathbb{K}^*}$
   - $x\mathbb{R}^+ = \{y \in \mathbb{K}^*; y = xh, h \in \mathbb{R}^+\} = \{y \in \mathbb{K}^*; \operatorname{Arg} y = \operatorname{Arg} x\}$;
   - $x\mathbb{R}^+ = y\mathbb{R}^+ \Leftrightarrow \frac{y}{x} \in \mathbb{R}^+ \Leftrightarrow y = xh, h \in \mathbb{R}^+ \Leftrightarrow \operatorname{Arg} y = \operatorname{Arg} x$.

c) $G/H = \mathbb{R}^*/\{1, -1\} = \{x\{1, -1\}\}_{x \in \mathbb{R}^*} = \{\{x, -x\}\}_{x \in \mathbb{R}^*}$, tj. $(\mathbb{R}^*/\{1, -1\}, \cdot) \cong (\mathbb{R}^+, \cdot)$.

d) $G/H = \mathbb{K}/\mathbb{R} = \{x + \mathbb{R}\}_{x \in \mathbb{K}} = \{y \in \mathbb{K}; y = x + h, h \in \mathbb{R}\} = \{y \in \mathbb{K}; y - x = h, h \in \mathbb{R}\} =$
   $= \{y \in \mathbb{K}; y - x \in \mathbb{R}\} = \{y \in \mathbb{K}; \operatorname{Im} y = \operatorname{Im} x\}$, tj. $(\mathbb{K}/\mathbb{R}, +) \cong (\mathbb{R}, +)$.

e) $G/H = \mathbb{R}^*/\mathbb{R}^+ = \{x\mathbb{R}^+\}_{x \in \mathbb{R}^*} = \{y \in \mathbb{R}^*; y = xh, h \in \mathbb{R}^+\} = \{y \in \mathbb{R}^*; \frac{y}{x} \in \mathbb{R}^+\}$
   $= \{y \in \mathbb{R}^*; \operatorname{sgn} y = \operatorname{sgn} x\}$, tj. $\mathbb{R}^*/\mathbb{R}^+ = \{\mathbb{R}^+, \mathbb{R}^-\}$.

Příklad 4. 1. 3:
Určete faktorovou grupu G/H, jestliže:

a) $G = (\mathbb{Z}_{16}, \oplus)$, $H = [\overline{4}]$;
b) $G = (\mathbb{Z}_{12}, \oplus)$, $H = (\{\overline{x} \in \mathbb{Z}_{12};\ \overline{x} = 3 \times \overline{k},\ \overline{k} \in \mathbb{Z}_{12}\}, \oplus)$;
c) $G = ([5], +)$, $H = ([20], +)$.

Řešení:
Stačí hledat např. levé třídy rozkladu, protože všechny uvedené struktury jsou komutativní.

a) $G = (\mathbb{Z}_{16}, \oplus)$, $H = [\overline{4}] = (\{\overline{0}, \overline{4}, \overline{8}, \overline{12}\}, \oplus)$;
$G/H = \mathbb{Z}_{16}/[\overline{4}] = \{\overline{x} \oplus [\overline{4}]\}_{\overline{x} \in \mathbb{Z}16} = \{\overline{x} \oplus \{\overline{0}, \overline{4}, \overline{8}, \overline{12}\}\}_{\overline{x} \in \mathbb{Z}16}$.
Počet rozkladových tříd, tj. index $[G : H] = 4$ ($|G| = |H| \cdot [G : H]$, kde $|G| = 16$, $|H| = 4$).
- $\overline{x} = \overline{0}$: $\overline{0} + H = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}\} = H$,
- $\overline{x} = \overline{1}$: $\overline{1} + H = \{\overline{1}, \overline{5}, \overline{9}, \overline{13}\} = H_1$,
- $\overline{x} = \overline{2}$: $\overline{2} + H = \{\overline{2}, \overline{6}, \overline{10}, \overline{14}\} = H_2$,
- $\overline{x} = \overline{3}$: $\overline{3} + H = \{\overline{3}, \overline{7}, \overline{11}, \overline{15}\} = H_3$.

Tedy $(G/H, \oplus) = (\{H, H_1, H_2, H_3\}, \oplus)$.

b) $G = (\mathbb{Z}_{12}, \oplus)$, $H = (\{\overline{x} \in \mathbb{Z}_{12};\ \overline{x} = 3 \times \overline{k},\ \overline{k} \in \mathbb{Z}_{12}\}, \oplus) = (\{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}, \oplus) = [\overline{3}]$;
$G/H = \mathbb{Z}_{12}/[\overline{3}] = \{\overline{x} \oplus [\overline{3}]\}_{\overline{x} \in \mathbb{Z}12} = \{\overline{x} \oplus \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}\}_{\overline{x} \in \mathbb{Z}12}$; $[G : H] = 3$.
- $\overline{x} = \overline{0}$: $\overline{0} + H = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = H$,
- $\overline{x} = \overline{1}$: $\overline{1} + H = \{\overline{1}, \overline{4}, \overline{7}, \overline{10}\} = H_1$,
- $\overline{x} = \overline{2}$: $\overline{2} + H = \{\overline{2}, \overline{5}, \overline{8}, \overline{11}\} = H_2$.

$(G/H, \oplus) = (\{H, H_1, H_2\}, \oplus)$.

c) $G = ([5], +) = (\{x \in \mathbb{Z};\ x = 5k,\ k \in \mathbb{Z}\}, +)$, $H = ([20], +) = (\{x \in \mathbb{Z};\ x = 20l,\ l \in \mathbb{Z}\}, +)$;
$G/H = [5]/[20] = \{x + [20]\}_{x \in [5]}$.
- $x + [20] = \{y \in \mathbb{Z};\ y = x + h,\ h \in [20]\} = \{y \in \mathbb{Z};\ y = 5k + 20l,\ k, l \in \mathbb{Z}\} =$
$= \{y \in \mathbb{Z};\ y = 5(k + 4l),\ k, l \in \mathbb{Z}\}$;
- pro $k = 0$ je $x = 0$: $0 + [20] = H$,
- pro $k = 1$ je $x = 5$: $5 + [20] = \{y \in \mathbb{Z};\ y = 5 + 20l,\ l \in \mathbb{Z}\} = H_1$,
- pro $k = 2$ je $x = 10$: $10 + [20] = \{y \in \mathbb{Z};\ y = 10 + 20l,\ l \in \mathbb{Z}\} = H_2$,
- pro $k = 3$ je $x = 15$: $15 + [20] = \{y \in \mathbb{Z};\ y = 15 + 20l,\ l \in \mathbb{Z}\} = H_3$.

Tedy $(G/H, +) = (\{H, H_1, H_2, H_3\}, +)$.

Příklad 4. 1. 4(∗):
Nalezněte všechny normální podgrupy multiplikativní grupy šestých odmocnin z jedné. Dále určete všechny faktorové grupy podle těchto podgrup.

Řešení:
Využijeme příkladu 3. 1. 9; $B = (\{x \in \mathbb{K};\ x^6 - 1 = 0\}, \cdot) = (\{x_1, x_2, x_3, x_4, x_5, x_6\}, \cdot)$.
Podgrupy: $B = [x_5] = [x_6]$, $B_1 = [x_1] = (\{x_1\}, \cdot)$, $B_2 = [x_2] = [x_3] = (\{x_1, x_2, x_3\}, \cdot)$,
$B_3 = [x_4] = (\{x_1, x_4\}, \cdot)$.

Protože B je cyklická, a tudíž komutativní grupa, jsou všechny její podgrupy normální.

- $B/B = \{x \cdot B\}_{x \in B} = \{B\}$,
- $B/B_1 = \{x \cdot B_1\}_{x \in B} = \{x \cdot \{x_1\}\}_{x \in B} = \{\{x\}\}_{x \in B}$,
- $B/B_2 = \{x \cdot B_2\}_{x \in B} = \{x \cdot \{x_1, x_2, x_3\}\}_{x \in B} = \{\{x_1, x_2, x_3\}, \{x_4, x_5, x_6\}\}$.
- B/B_3:
  - $[B : B_3] = 3$ ($|B| = 6$, $|B_3| = 2$),

- $x_1 \cdot B_3 = x_1 \cdot \{x_1, x_4\} = \{x_1, x_4\} = B_3$,
- $x_2 \cdot B_3 = x_2 \cdot \{x_1, x_4\} = \{x_2, x_6\}$,
- $x_3 \cdot B_3 = x_3 \cdot \{x_1, x_4\} = \{x_3, x_5\}$.

Tedy $B/B_3 = \{\{x_1, x_4\}, \{x_2, x_6\}, \{x_3, x_5\}\}$.

Příklad 4. 1. 5$(*)$**:**

Zjistěte, zda H je normální podgrupou grupy G, jestliže $G = (\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R});\ a \neq 0\}, \cdot)$, $H = (\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})\}, \cdot)$. Pokud ano, určete G/H.

Řešení:

Platí: $N \trianglelefteq G \Leftrightarrow (\forall\, g \in G)\ (\forall\, n \in N)\ \ gng^{-1} \in N$.

Musíme tedy ověřit, zda platí: $(\forall\, A \in G)\ (\forall\, B \in H)\ \ A \cdot B \cdot A^{-1} \in H$:

$A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, $A^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}$

$$A \cdot B \cdot A^{-1} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ax+b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & ax \\ 0 & 1 \end{pmatrix} \in H.$$

Tedy $H \trianglelefteq G$.

- $G/H = \{A \cdot H\}_{A \in G}$
  - $A \cdot H = \{Y \in G;\ Y = A \cdot B,\ B \in H\} = \{Y \in G;\ Y = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ a \neq 0\} =$
    $= \{Y \in G;\ Y = \begin{pmatrix} a & ax+b \\ 0 & 1 \end{pmatrix},\ a \neq 0\}$.

Příklad 4. 1. 6$(*)$**:**

Nechť $G = (\{A \in M_n(\mathbb{R});\ \det A \neq 0\}, \cdot)$, $H = (\{B \in M_n(\mathbb{R});\ \det B > 0\}, \cdot)$.

Dokažte, že G/H je cyklická grupa řádu 2.

Řešení:

$G/H = \{A \cdot H\}_{A \in G}$

- $A \cdot H = \{Y \in G;\ Y = A \cdot B,\ B \in H\} = \{Y \in G;\ \det Y = \det A \cdot \det B,\ B \in H\}$
  - je-li $\det A > 0$, pak $A \cdot H = H$,
  - je-li $\det A < 0$, pak $A \cdot H = G - H$.

Tedy $(G/H, \cdot) = (\{H, G - H\}, \cdot) \cong (\mathbb{Z}_2, \oplus)$, což je cyklická grupa řádu 2.

Příklad 4. 1. 7:

Nechť $(G, \cdot)$ je cyklická grupa řádu 9. Určete:

a) řády všech prvků;
b) podgrupu H řádu 3;
c) $[G : H]$;
d) G/H.

Řešení:

$G = [a] = (\{1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}, \cdot)$.

a) Řády prvků určíme dvěma způsoby:
   - Hledáme $n \in \mathbb{Z}^+$ nejmenší takové, že $x^n = 1$, kde $x \in G$:

     $o(1) = 1$, $o(a) = 9$ $(a^9 = 1)$, $o(a^2) = 9$ $((a^2)^9 = 1)$, $o(a^3) = 3$ $((a^3)^3 = 1)$, $o(a^4) = 9$ $((a^4)^9 = 1)$, $o(a^5) = 9$ $((a^5)^9 = 1)$, $o(a^6) = 3$ $((a^6)^3 = 1)$, $o(a^7) = 9$ $((a^7)^9 = 1)$, $o(a^8) = 9$ $((a^8)^9 = 1)$.

- $nsd(k, 9) = 1 \Leftrightarrow k = 1, 2, 4, 5, 7, 8$
  $G = [a] = [a^2] = [a^4] = [a^5] = [a^7] = [a^8]$.
  Tedy $o(a) = o(a^2) = o(a^4) = o(a^5) = o(a^7) = o(a^8) = 9$, neboť G je řádu 9.
- Podgrupy:
  $d \mid 9 \Leftrightarrow d = 1, 3, 9$
  $H_1 = G = [a]$, $H_2 = [a^3] = (\{1, a^3, a^6\}, \cdot) = [a^6]$, tedy $o(a^3) = o(a^6) = 3$,
  $H_3 = [a^9] = [1] = (\{1\}, \cdot)$, tedy $o(1) = 1$.

b) $H = H_2$ (viz a)).

c) $|G| = 9$, $|H| = 3$, tedy $[G : H] = 3$.

d) $G/H = [a]/[a^3] = \{x \cdot [a^3]\}_{x \in [a]}$.
- $x = 1$: $1 \cdot [a^3] = [a^3] = \{1, a^3, a^6\}$,
- $x = a$: $a \cdot [a^3] = a \cdot \{1, a^3, a^6\} = \{a, a^4, a^7\}$,
- $x = a^2$: $a^2 \cdot [a^3] = a^2 \cdot \{1, a^3, a^6\} = \{a^2, a^5, a^8\}$.

$G/H = \{\{1, a^3, a^6\}, \{a, a^4, a^7\}, \{a^2, a^5, a^8\}\}$.

Příklad 4. 1. 8:
Nechť $(G, \cdot)$ je grupa, kde $G = \{a, b, c, d, e, f\}$ a operace „$\cdot$“ je dána tabulkou:

$\cdot$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	e	f	c	d
c	c	f	a	e	d	b
d	d	e	f	a	b	c
e	e	d	b	c	f	a
f	f	c	d	b	a	e

a) Nalezněte všechny podgrupy grupy G.
b) Určete, které z nich jsou normální.
c) Určete faktorové grupy podle těchto normálních podgrup.

Řešení:

a) Podgrupy:
$H_1 = (G, \cdot)$, $H_2 = (\{a\}, \cdot)$, $H_3 = (\{a, b\}, \cdot)$, $H_4 = (\{a, c\}, \cdot)$, $H_5 = (\{a, d\}, \cdot)$,
$H_6 = (\{a, e, f\}, \cdot)$.

b) Normální podgrupy:
$H_1 \trianglelefteq G$, $H_2 \trianglelefteq G$ (triviální podgrupy); $H_6 \trianglelefteq G$, neboť $[G : H_6] = 2$ (viz věta 4. 11.)
U podgrup H_3, H_4, H_5 zjistíme, zda se rovnají rozklady na levé a pravé třídy:
- H_3: $c \cdot H_3 = c \cdot \{a, b\} = \{c, f\}$, $H_3 \cdot c = \{a, b\} \cdot c = \{c, e\}$;
  $c \cdot H_3 \neq H_3 \cdot c \Longrightarrow H_3 \not\trianglelefteq G$.
- H_4: $b \cdot H_4 = b \cdot \{a, c\} = \{b, e\}$, $H_4 \cdot b = \{a, c\} \cdot b = \{b, f\}$;
  $b \cdot H_4 \neq H_4 \cdot b \Longrightarrow H_4 \not\trianglelefteq G$.
- H_5: $e \cdot H_5 = e \cdot \{a, d\} = \{e, c\}$, $H_5 \cdot e = \{a, d\} \cdot e = \{e, b\}$;
  $e \cdot H_5 \neq H_5 \cdot e \Longrightarrow H_5 \not\trianglelefteq G$.

c) Faktorové grupy:
- $G/H_1 = G/G = \{x \cdot G\}_{x \in G} = \{G\}$,
- $G/H_2 = G/\{a\} = \{x \cdot \{a\}\}_{x \in G} = \{\{x\}\}_{x \in G}$,
- $G/H_6 = \{H_6, G - H_6\} = \{\{a, e, f\}, \{b, c, d\}\}$.

Příklad 4. 1. 9:
Nechť $(G, \cdot)$ je grupa. Dokažte, že prvky, které jsou v grupě G konjugované, mají stejný řád.

Řešení:
Pokud je $x \sim y$, tj. $y = g^{-1}xg$ pro nějaké $g \in G$, pak také $x^n \sim y^n$ pro libovolné $n \in \mathbb{Z}^+$, protože $y^n = g^{-1}xgg^{-1}xg\ldots g^{-1}xg = g^{-1}x^ng$. Nechť $x \in G$ je prvek řádu n. Tedy $n \in \mathbb{Z}^+$ nejmenší takové, že $1 \sim x^n$ ($x^n = g^{-1}1g = g^{-1}g = 1$, pro každé $g \in G$). Protože $1 \sim x^n$ a zároveň $x^n \sim y^n$, je také $1 \sim y^n$ (relace „~“ je tranzitivní), neboli $y^n = 1$. Kdyby existovalo $m \in \mathbb{Z}^+$, $m < n$, takové, že $y^m = 1$, pak by platilo:
$x^m \sim y^m \Longrightarrow (\exists g \in G)\ \ x^m = g^{-1}y^mg = g^{-1}1g = g^{-1}g = 1$, což je spor s tím, že $o(x) = n$. Tedy takové m neexistuje, a proto také $o(y) = n$.

Příklad 4. 1. 10:
V grupě $(\mathbb{Z}, +)$ definujme relaci R takto: $(\forall\, x, y \in \mathbb{Z})\ \ xRy \Leftrightarrow (\exists\, k \in \mathbb{Z})\ \ x = y + 6k$.
Zjistěte, zda R je kongruence v grupě $(\mathbb{Z}, +)$. Pokud ano, určete faktorovou grupu $\mathbb{Z}/R$.

Řešení:

- $(\forall\, x \in \mathbb{Z})\ \ x = x + 6\cdot 0,\ 0 \in \mathbb{Z}$, tj. xRx;
  $(\forall\, x, y \in \mathbb{Z})\ \ xRy \Longrightarrow (\exists\, k \in \mathbb{Z})\ \ x = y + 6k \Longrightarrow y = x + 6(-k),\ -k \in \mathbb{Z}$, tj. yRx;
  $(\forall\, x, y, z \in \mathbb{Z})\ \ xRy \wedge yRz \Longrightarrow (\exists\, k, l \in \mathbb{Z})\ \ x = y + 6k \wedge y = z + 6l \Longrightarrow x = z + 6l + 6k = z + 6(l + k) = z + 6t,\ t \in \mathbb{Z}$, tj. xRz.

  Tedy R je ekvivalence.

  $(\forall\, x_1, x_2, y_1, y_2 \in \mathbb{Z})\ \ x_1Rx_2 \wedge y_1Ry_2 \Longrightarrow (\exists\, k, l \in \mathbb{Z})\ \ x_1 = x_2 + 6k \wedge y_1 = y_2 + 6l \Longrightarrow$
  $\Longrightarrow x_1 + y_1 = x_2 + 6k + y_2 + 6l = x_2 + y_2 + 6(k + l) = x_2 + y_2 + 6t,\ t \in \mathbb{Z} \Longrightarrow$
  $\Longrightarrow (x_1 + y_1)R(x_2 + y_2)$, tj. R je kongruence.

- $\mathbb{Z}/R = \{\square Rx\}_{x \in \mathbb{Z}}$
  $\square Rx = \{y \in \mathbb{Z};\ yRx\} = \{y \in \mathbb{Z};\ y = x + 6k,\ k \in \mathbb{Z}\}$.
  - $x = 0$: $\square R0 = \{y \in \mathbb{Z};\ y = 6k,\ k \in \mathbb{Z}\}$,
  - $x = 1$: $\square R1 = \{y \in \mathbb{Z};\ y = 1 + 6k,\ k \in \mathbb{Z}\}$,
  - $x = 2$: $\square R2 = \{y \in \mathbb{Z};\ y = 2 + 6k,\ k \in \mathbb{Z}\}$,
  - $x = 3$: $\square R3 = \{y \in \mathbb{Z};\ y = 3 + 6k,\ k \in \mathbb{Z}\}$,
  - $x = 4$: $\square R4 = \{y \in \mathbb{Z};\ y = 4 + 6k,\ k \in \mathbb{Z}\}$,
  - $x = 5$: $\square R5 = \{y \in \mathbb{Z};\ y = 5 + 6k,\ k \in \mathbb{Z}\}$.

  Tedy $\mathbb{Z}/R = \{\square R0, \square R1, \square R2, \square R3, \square R4, \square R5\}$.

3. 4. 2. Příklady k procvičení

Příklad 4. 2. 1:
Určete faktorovou grupu G/H, jestliže $G = (\mathbb{R}, +)$, $H = (\mathbb{Z}, +)$.

Příklad 4. 2. 2:
Určete faktorovou grupu G/H, jestliže:
a) $G = (\mathbb{Z}_8, \oplus)$, $H = (\{\overline{0}, \overline{4}\}, \oplus)$ b) $G = (\mathbb{Z}, +)$, $H = ([2], +)$.

Příklad 4. 2. 3:
Zjistěte, zda H je normální podgrupou grupy G, jestliže $G = (\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R});\ a \neq 0\}, \cdot)$, $H = (\{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})\}, \cdot)$. Pokud ano, určete G/H.

3. 5. Permutační grupy

3. 5. 1. Řešené příklady

Příklad 5. 1. 1:

Ukažte, že množina $P = \{\Pi_1, \Pi_2, \Pi_3, \Pi_4\}$, kde $\Pi_1 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$, $\Pi_2 = \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$, $\Pi_3 = \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$, $\Pi_4 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$ jsou permutace množiny $M = \{1, 2, 3, 4\}$, je spolu s operací skládání zobrazení komutativní grupou.

Řešení:

Sestavíme Cayleyho tabulku:

$\circ$	Π_1	Π_2	Π_3	Π_4
Π_1	Π_1	Π_2	Π_3	Π_4
Π_2	Π_2	Π_1	Π_4	Π_3
Π_3	Π_3	Π_4	Π_1	Π_2
Π_4	Π_4	Π_3	Π_2	Π_1

- Protože skládání zobrazení je asociativní, je z Cayleyho tabulky zřejmé, že $(P, \circ)$ je komutativní grupa.

Příklad 5. 1. 2:

Vyjádřete permutaci Π ve tvaru součinu nezávislých cyklů, určete její řád, paritu, inverzní permutaci, jestliže:

a) $\Pi = \begin{pmatrix}1&2&3&4&5&6&7\\3&7&5&6&1&2&4\end{pmatrix} \in S_7$;

b) $\Pi = \begin{pmatrix}1&2&3&4&5&6&7&8\\4&6&5&1&7&2&3&8\end{pmatrix} \in S_8$.

Řešení:

a)
- $\Pi = (1, 3, 5)\cdot(2, 7, 4, 6)$.
- $o(\Pi) = nsn(3, 4) = 12$.
- Paritu určíme třemi způsoby:
  1) $\Pi = (1, 5)\cdot(1, 3)\cdot(2, 6)\cdot(2, 4)\cdot(2, 7)$, Π je součinem pěti transpozic, tedy lichá;
  2) počet inverzí: 13;
  3) sgn $\Pi = (-1)^{k-1}$, je-li Π cyklus délky k; tedy sgn $\Pi = (-1)^2\cdot(-1)^3 = -1$.
- $\Pi^{-1} = \begin{pmatrix}1&2&3&4&5&6&7\\5&6&1&7&3&4&2\end{pmatrix} = (1, 5, 3)\cdot(2, 6, 4, 7)$.

b)
- $\Pi = (1, 4)\cdot(2, 6)\cdot(3, 5, 7)$.
- $o(\Pi) = nsn(2, 2, 3) = 6$.
- Parita:
  1) $\Pi = (1, 4)\cdot(2, 6)\cdot(3, 7)\cdot(3, 5)$, Π je součinem čtyř transpozic, tedy sudá;
  2) počet inverzí: 12;
  3) sgn $\Pi = (-1)\cdot(-1)\cdot(-1)^2 = 1$.
- $\Pi^{-1} = \begin{pmatrix}1&2&3&4&5&6&7&8\\4&6&7&1&3&2&5&8\end{pmatrix} = (1, 4)\cdot(2, 6)\cdot(3, 7, 5)$.

Příklad 5. 1. 3:

Nechť $\Pi = \begin{pmatrix}1&2&3&4&5&6&7\\2&4&5&7&6&3&1\end{pmatrix} \in S_7$. Určete:

a) Π^{999};

b) Π^{5627}.

Řešení:
$\Pi = (1, 2, 4, 7)\cdot(3, 5, 6)$, takže $o(\Pi) = 12$, tj. $\Pi^{12} = I$, tudíž $(\Pi^{12})^k = I$, $k \in \mathbb{Z}$.
Pak $\Pi^l = \Pi^{12q+r} = (\Pi^{12})^q \cdot \Pi^r = \Pi^r$, $0 \leq r < 12$.

a) $\Pi^{999} = \Pi^{12\cdot 83+3} = \Pi^3$;
$\Pi^2 = (1, 4)\cdot(2, 7)\cdot(3, 6, 5)$, $\Pi^3 = (1, 7, 4, 2)$.

b) $\Pi^{5627} = \Pi^{12\cdot 468+11} = \Pi^{11}$;
$\Pi^{12} = \Pi \cdot \Pi^{11} = I \Longrightarrow \Pi^{11} = \Pi^{-1} = (7, 4, 2, 1)\cdot(6, 5, 3)$.

Příklad 5. 1. 4:
Jsou dány permutace $A = (1, 3)\cdot(2, 5, 4)$, $B = (1, 3, 5, 2)$ z grupy S_5. Určete:

a) $A^{121} \cdot B^{82}$;
b) $A^{14} \cdot B^{-3}$.

Řešení:
$o(A) = 6$, $o(B) = 4$

a) $A^{121} \cdot B^{82} = A^{6\cdot 20+1} \cdot B^{4\cdot 20+2} = A \cdot B^2$,
$B^2 = (1, 5)\cdot(3, 2)$;
$A \cdot B^2 = (1, 2)\cdot(3, 5, 4)$.

b) $A^{14} \cdot B^{-3} = A^{6\cdot 2+2} \cdot (B^3)^{-1} = A^2 \cdot (B^3)^{-1}$,
$A^2 = (2, 4, 5)$, $B^3 = (1, 2, 5, 3)$, $(B^3)^{-1} = (3, 5, 2, 1)$,
$A^2 \cdot (B^3)^{-1} = (2, 4)\cdot(5, 1, 3)$.

Příklad 5. 1. 5($*$):
Určete, jaký nejvyšší řád mohou mít permutace z grupy S_8 a S_{14}.

Řešení:
Permutace musíme rozložit v součin nezávislých cyklů tak, aby nejmenší společný násobek jejich délek byl co největší.
V grupě S_8: $nsn(3, 5) = 15$; v grupě S_{14}: $nsn(3, 4, 7) = 84$.
Tedy permutace v grupě S_8 mohou být až řádu 15, v grupě S_8 až řádu 84.

Příklad 5. 1. 6:
Určete cyklickou podgrupu grupy S_5 generovanou permutací:

a) $\Pi = (1, 3)\cdot(2, 5, 4)$;
b) $\Pi = (1, 4)\cdot(3, 5)$;
c) $\Pi = (1, 2, 3, 4)$.

Řešení:

a) Hledáme $H = [\Pi] = (\{I, \Pi, \Pi^2, \Pi^3, \Pi^4, \Pi^5\}, \cdot)$, neboť $o(\Pi) = 6$.
$\Pi = (1, 3)\cdot(2, 5, 4)$, $\Pi^2 = (2, 4, 5)$, $\Pi^3 = (1, 3)$, $\Pi^4 = (2, 5, 4)$, $\Pi^5 = (1, 3)\cdot(2, 4, 5)$, $\Pi^6 = I$.

b) $o(\Pi) = 2 \Longrightarrow H = [\Pi] = (\{I, \Pi\}, \cdot)$.

c) $o(\Pi) = 4 \Longrightarrow H = [\Pi] = (\{I, \Pi, \Pi^2, \Pi^3\}, \cdot)$.
$\Pi = (1, 2, 3, 4)$, $\Pi^2 = (1, 3)\cdot(2, 4)$, $\Pi^3 = (1, 4, 3, 2)$, $\Pi^4 = I$.

Příklad 5. 1. 7:
Řešte v S_6 rovnici: $A \cdot X \cdot B = C$. Přitom $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 2 & 3 & 6 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 5 & 4 & 3 & 1 \end{pmatrix}$,
$C = (1, 6, 4, 3)\cdot(2, 5)$.

Řešení:
A = (1, 5, 3)·(2, 4), B = (1, 2, 6)·(3, 5), C = (1, 6, 4, 3)·(2, 5).
$A \cdot X \cdot B = C$
$X \cdot B = A^{-1} \cdot C$
$X = A^{-1} \cdot C \cdot B^{-1}$
A^{-1} = (3, 5, 1)·(2, 4), B^{-1} = (6, 2, 1)·(3, 5),
X = (3, 1, 6, 4)·(5, 2).

Příklad 5. 1. 8:
Určete permutaci $X = A \cdot B^2 \cdot C \cdot A^2$ a její řád, jestliže A = (2, 3, 4), B = (1, 3, 5, 7, 6, 4, 2), C = (1, 7, 3, 5) jsou cykly z grupy S_7.

Řešení:
A^2 = (2, 4, 3), B^2 = (1, 5, 6, 2, 3, 7, 4),
$X = A \cdot B^2 \cdot C \cdot A^2$ = (3, 7)·(4, 5, 6),
$o(X) = nsn(2, 3) = 6$.

Příklad 5. 1. 9:
Určete řád permutací:
A = (1, 2, 4, 5)·(3, 7, 8)·(6, 9), B = (1, 2, 4, 5, 3, 6, 7, 9)·(3, 7, 8)·(6, 2, 9) ∈ S_9.

Řešení:
Permutace A je součinem navzájem nezávislých cyklů, tedy $o(A) = nsn(4, 3, 2) = 12$.
Permutaci B musíme nejprve rozložit v součin nezávislých cyklů:
B = (1, 9)·(2, 4, 5, 7, 6, 8, 3), takže $o(B) = nsn(2, 7) = 14$.

Příklad 5. 1. 10:
Dokažte, že daná permutace je vždy sudá.
a) $\Pi = A^{10} \cdot B^{13} \cdot C^{18} \cdot B^{15}$;
b) $\Pi = (A^3 \cdot B^{-17})^{18} \cdot A^{10}$.

Řešení:
Využijeme toho, že sgn (Π^n) = sgn^n Π, a tedy jakákoli permutace umocněná na sudé číslo je sudá.
a) sgn Π = sgn $(A^{10} \cdot B^{13} \cdot C^{18} \cdot B^{15})$ = sgn A^{10} · sgn B^{13} · sgn C^{18} · sgn B^{15} =
= 1 · sgn B^{13} · 1 · sgn B^{15} = sgn $(B^{13} \cdot B^{15})$ = sgn (B^{28}) = 1.
Tím je tvrzení dokázáno.
b) $\Pi = (A^3 \cdot B^{-17})^{18} \cdot A^{10} = A^{54} \cdot B^{-306} \cdot A^{10} = A^{54} \cdot (B^{306})^{-1} \cdot A^{10}$,
sgn Π = sgn $(A^{54} \cdot (B^{306})^{-1} \cdot A^{10})$ = sgn A^{54} · sgn $(B^{306})^{-1}$ · sgn A^{10} =
= sgn A^{54} · sgn B^{306} · sgn A^{10} = sgn A^{54} · 1 · sgn A^{10} = sgn $(A^{54} \cdot A^{10})$ =
= sgn A^{64} = 1.

Poznámka:
Použili jsme definici 5. 2., větu 5. 6.

Příklad 5. 1. 11:
V grupě S_5 najděte permutaci X takovou, že (1, 3)·(2, 4, 5)· X ·(1, 4) = I.

Řešení:
Obecně: $A \cdot B \cdot X \cdot C = I$
$B \cdot X \cdot C = A^{-1}$
$X \cdot C = B^{-1} \cdot A^{-1}$
$X = B^{-1} \cdot A^{-1} \cdot C^{-1}$

A^{-1} = (1, 3), B^{-1} = (5, 4, 2), C^{-1} = (1, 4),
X = (5, 4, 2)·(1, 3)·(1, 4) = (5, 1, 3, 4, 2).

Příklad 5. 1. 12:
Určete podgrupu grupy S_4 generovanou množinou M = {(1, 2), (1, 4)}.

Řešení:
Nalezneme nejmenší podgrupu grupy S_4, která obsahuje množinu M. Kromě identity I a generátorů musíme do [M] zahrnout další prvky, abychom obdrželi grupu:

- (1, 2)·(1, 4) = (1, 2, 4),
- (1, 2)·(1, 2, 4) = (1, 4),
- (1, 4)·(1, 2, 4) = (4, 2),
- (1, 2, 4)·(1, 2, 4) = (1, 4, 2).

Dále už nemusíme skládat, protože jsme již vypsali všechny možnosti.
Tedy [M] = ({I, (1, 2), (1, 4), (4, 2), (1, 2, 4), (1, 4, 2)}, ·).
Skutečně jde o podgrupu v S_4, neboť M je uzavřená vzhledem k operaci „·“, neutrálním prvkem je I a ke každému prvku existuje prvek inverzní (každý z prvků I, (1, 2), (1, 4), (4, 2) je sám k sobě inverzní; prvky (1, 2, 4) a (1, 4, 2) jsou navzájem inverzní).

Příklad 5. 1. 13:

a) Nalezněte všechny podgrupy grupy S_3.
b) Určete, které z nich jsou normální.
c) Určete faktorové grupy podle těchto normálních podgrup.

Řešení:
$S_3 = (\{\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Pi_5, \Pi_6\}, \cdot)$, kde $\Pi_1 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $\Pi_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $\Pi_3 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$,
$\Pi_4 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $\Pi_5 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, $\Pi_6 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$.
Sestavíme Cayleyho tabulku, z níž určíme podgrupy.

·	Π_1	Π_2	Π_3	Π_4	Π_5	Π_6
Π_1	Π_1	Π_2	Π_3	Π_4	Π_5	Π_6
Π_2	Π_2	Π_3	Π_1	Π_6	Π_4	Π_5
Π_3	Π_3	Π_1	Π_2	Π_5	Π_6	Π_4
Π_4	Π_4	Π_5	Π_6	Π_1	Π_2	Π_3
Π_5	Π_5	Π_6	Π_4	Π_3	Π_1	Π_2
Π_6	Π_6	Π_4	Π_5	Π_2	Π_3	Π_1

a) Podgrupy:
$H_1 = S_3$, $H_2 = (\{\Pi_1\}, \cdot)$, $H_3 = (\{\Pi_1, \Pi_4\}, \cdot)$, $H_4 = (\{\Pi_1, \Pi_5\}, \cdot)$, $H_5 = (\{\Pi_1, \Pi_6\}, \cdot)$,
$H_6 = (\{\Pi_1, \Pi_2, \Pi_3\}, \cdot)$.

b) Normální podgrupy:
$H_1 \trianglelefteq S_3$, $H_2 \trianglelefteq S_3$ (triviální podgrupy), $H_6 \trianglelefteq S_3$ (neboť $[S_3 : H_6] = 2$).
U podgrup H_3, H_4, H_5 zjistíme, zda se rovnají rozklady na levé a pravé třídy:
- H_3: $\Pi_2 \cdot H_3 = \Pi_2 \cdot \{\Pi_1, \Pi_4\} = \{\Pi_2, \Pi_6\}$, $H_3 \cdot \Pi_2 = \{\Pi_1, \Pi_4\} \cdot \Pi_2 = \{\Pi_2, \Pi_5\}$;
  $\Pi_2 \cdot H_3 \neq H_3 \cdot \Pi_2 \Longrightarrow H_3 \not\trianglelefteq S_3$.
- H_4: $\Pi_3 \cdot H_4 = \Pi_3 \cdot \{\Pi_1, \Pi_5\} = \{\Pi_3, \Pi_6\}$, $H_4 \cdot \Pi_3 = \{\Pi_1, \Pi_5\} \cdot \Pi_3 = \{\Pi_3, \Pi_4\}$;
  $\Pi_3 \cdot H_4 \neq H_4 \cdot \Pi_3 \Longrightarrow H_4 \not\trianglelefteq S_3$.

- H_5: $\Pi_4 \cdot H_5 = \Pi_4 \cdot \{\Pi_1, \Pi_6\} = \{\Pi_4, \Pi_3\}$, $H_5 \cdot \Pi_4 = \{\Pi_1, \Pi_6\} \cdot \Pi_4 = \{\Pi_4, \Pi_2\}$;
  $\Pi_4 \cdot H_5 \neq H_5 \cdot \Pi_4 \Longrightarrow H_4 \not\trianglelefteq S_3$.

c) Faktorové grupy:
- $S_3/H_1 = S_3/\ S_3 = \{\Pi \cdot S_3;\ \Pi \in S_3\} = \{S_3\}$,
- $S_3/H_2 = S_3/\{\Pi_1\} = \{\Pi \cdot \{\Pi_1\};\ \Pi \in S_3\} = \{\{\Pi\};\ \Pi \in S_3\}$,
- $S_3/H_6 = \{H_6, S_3 - H_6\} = \{\{\Pi_1, \Pi_2, \Pi_3\}, \{\Pi_4, \Pi_5, \Pi_6\}\}$.

Příklad 5. 1. 14:
Rozhodněte, zda podgrupa H generovaná cyklem $A = (1, 2, 3)$ je normální podgrupa v S_4.

Řešení:
$H = [A] = (\{I, A, A^2\}, \cdot) = (\{I, (1, 2, 3), (1, 3, 2)\}, \cdot)$
$H \trianglelefteq S_4 \Leftrightarrow (\forall\, X \in S_4)\ (\forall\, Y \in H)\ \ X \cdot Y \cdot X^{-1} \in H.$
Např. $(1, 2, 4)\cdot(1, 2, 3)\cdot(4, 2, 1) = (1, 3, 4) \notin H$, tudíž $H \not\trianglelefteq S_4$.

3. 5. 2. Příklady k procvičení

Příklad 5. 2. 1:
Vyjádřete permutaci Π ve tvaru součinu nezávislých cyklů, určete její řád, paritu, inverzní permutaci, jestliže:

a) $\Pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 5 & 2 & 3 & 1 & 4 \end{pmatrix} \in S_7$;

b) $\Pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 1 & 3 & 5 & 7 & 2 & 6 \end{pmatrix} \in S_8$.

Příklad 5. 2. 2:
Nechť $\Pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 3 & 5 & 4 & 7 \end{pmatrix} \in S_7$. Určete:

a) Π^{68} b) Π^{136} c) Π^{1212}.

Příklad 5. 2. 3:
Jsou dány permutace $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix} \in S_5$.

a) Zapište tyto permutace jako součin navzájem nezávislých cyklů.
b) Určete permutaci $A \cdot B$.
c) Určete permutaci A^{15}.
d) Rozložte permutaci B na součin transpozic.

Příklad 5. 2. 4:
Jsou dány permutace $A, B, C \in S_9$, $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 7 & 8 & 1 & 4 & 2 & 6 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 5 & 2 & 6 & 3 & 7 & 4 & 9 \end{pmatrix}$,
$C = A \cdot B$.

a) Napište permutace A, B, C jako součin navzájem nezávislých cyklů.
b) Určete paritu permutací A, B, C.
c) Určete permutaci $D = A^{100} \cdot B^{100}$.

Příklad 5. 2. 5:
Nechť $D = A^7 \cdot B^8 \cdot A^9$. Určete paritu permutace D.

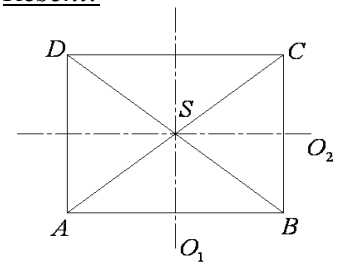
Příklad 5. 2. 6:
Rozhodněte, zda podgrupa generovaná transpozicí (1, 2) je normální podgrupou v S_3.

3. 6. Grupy symetrií

3. 6. 1. Řešené příklady

Příklad 6. 1. 1:
Sestavte Cayleyho tabulku pro grupu symetrií obdélníku a rozhodněte, zda je tato grupa komutativní.

Řešení:



Všechny symetrie můžeme popsat pomocí permutací:

$I = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$, $S = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$, $O_1 = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$, $O_2 = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$.

Cayleyho tabulka:

$\circ$	I	S	O_1	O_2
I	I	S	O_1	O_2
S	S	I	O_2	O_1
O_1	O_1	O_2	I	S
O_2	O_2	O_1	S	I

- Protože tabulka je souměrná podle hlavní diagonály, je grupa symetrií obdélníku komutativní.

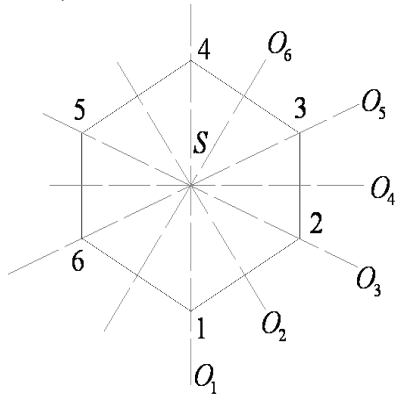
Poznámka:

1) Grupa symetrií obdélníku je izomorfní s grupou $(\mathbb{Z}_2 \times \mathbb{Z}_2, \oplus)$, která se nazývá Kleinova čtyřgrupa.
2) Každá čtyřprvková grupa je izomorfní s cyklickou grupou $(\mathbb{Z}_4, \oplus)$ nebo s grupou symetrií obdélníku. (Jde o důsledek Lagrangeovy věty.)

Příklad 6. 1. 2:
Nechť H je podgrupa grupy D_6, která ponechává vrchol číslo 2 na místě.

a) Určete rozklad na levé a pravé třídy podle podgrupy H.
b) Rozhodněte, zda H je normální podgrupou v D_6.

Řešení:
$D_6 = (\{I, R, R^2, R^3, R^4, R^5, O, O\circ R, O\circ R^2, O\circ R^3, O\circ R^4, O\circ R^5\}, \circ)$.



Jednotlivé symetrie vyjádříme pomocí permutací:

$I = \begin{pmatrix}1&2&3&4&5&6\\1&2&3&4&5&6\end{pmatrix}$, $R = \begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix}$, $R^2 = \begin{pmatrix}1&2&3&4&5&6\\3&4&5&6&1&2\end{pmatrix}$, $R^3 = \begin{pmatrix}1&2&3&4&5&6\\4&5&6&1&2&3\end{pmatrix}$,

$R^4 = \begin{pmatrix}1&2&3&4&5&6\\5&6&1&2&3&4\end{pmatrix}$, $R^5 = \begin{pmatrix}1&2&3&4&5&6\\6&1&2&3&4&5\end{pmatrix}$, $O_1 = O = \begin{pmatrix}1&2&3&4&5&6\\1&6&5&4&3&2\end{pmatrix}$, $O_2 = O\circ R = \begin{pmatrix}1&2&3&4&5&6\\2&1&6&5&4&3\end{pmatrix}$,

$O_3 = O\circ R^2 = \begin{pmatrix}1&2&3&4&5&6\\3&2&1&6&5&4\end{pmatrix}$, $O_4 = O\circ R^3 = \begin{pmatrix}1&2&3&4&5&6\\4&3&2&1&6&5\end{pmatrix}$, $O_5 = O\circ R^4 = \begin{pmatrix}1&2&3&4&5&6\\5&4&3&2&1&6\end{pmatrix}$,

$O_6 = O\circ R^5 = \begin{pmatrix}1&2&3&4&5&6\\6&5&4&3&2&1\end{pmatrix}$.

Tedy $H = (\{I, O\circ R^2\}, \circ)$.

a) Rozklad na levé třídy: $S = \{X\circ H; X \in D_6\}$.
Rozklad na pravé třídy: $S' = \{H\circ X; X \in D_6\}$.
Protože $|D_6| = 12$, $|H| = 2$, je $[D_6 : H] = 6$, tj. rozklady S, S' mají šest tříd.

- S:
  - $I\circ H = H = \{I, O\circ R^2\}$,
  - $O\circ H = O\circ\{I, O\circ R^2\} = \{O, R^2\}$,
  - $R\circ H = R\circ\{I, O\circ R^2\} = \{R, O\circ R\}$,
  - $R^3\circ H = R^3\circ\{I, O\circ R^2\} = \{R^3, O\circ R^5\}$,
  - $R^4\circ H = R^4\circ\{I, O\circ R^2\} = \{R^4, O\circ R^4\}$,
  - $R^5\circ H = R^5\circ\{I, O\circ R^2\} = \{R^5, O\circ R^3\}$.

  Tedy $S = \{\{I, O\circ R^2\}, \{O, R^2\}, \{R, O\circ R\}, \{R^3, O\circ R^5\}, \{R^4, O\circ R^4\}, \{R^5, O\circ R^3\}\}$.

- S':
  - $H\circ I = H = \{I, O\circ R^2\}$,
  - $H\circ O = \{I, O\circ R^2\}\circ O = \{O, R^4\}$,
  - $H\circ R = \{I, O\circ R^2\}\circ R = \{R, O\circ R^3\}$,
  - $H\circ R^3 = \{I, O\circ R^2\}\circ R^3 = \{R^3, O\circ R^5\}$,
  - $H\circ R^5 = \{I, O\circ R^2\}\circ R^5 = \{R^5, O\circ R\}$,
  - $H\circ R^2 = \{I, O\circ R^2\}\circ R^2 = \{R^2, O\circ R^4\}$.

  Tedy $S = \{\{I, O\circ R^2\}, \{O, R^4\}, \{R, O\circ R^3\}, \{R^3, O\circ R^5\}, \{R^5, O\circ R\}, \{R^2, O\circ R^4\}\}$.

b) $S \neq S' \Longrightarrow H \not\trianglelefteq D_6$.

Příklad 6. 1. 3(∗)**:**

a) Nalezněte všechny podgrupy grupy D_3.
b) Určete, které z nich jsou normální.
c) Určete faktorové grupy podle těchto normálních podgrup.

Řešení:
$D_3 = (\{I, R, R^2, O, O\circ R, O\circ R^2\}, \circ)$
Cayleyho tabulka:

$\circ$	I	R	R^2	O	$O\circ R$	$O\circ R^2$
I	I	R	R^2	O	$O\circ R$	$O\circ R^2$
R	R	R^2	I	$O\circ R^2$	O	$O\circ R$
R^2	R^2	I	R	$O\circ R$	$O\circ R^2$	O
O	O	$O\circ R$	$O\circ R^2$	I	R	R^2
$O\circ R$	$O\circ R$	$O\circ R^2$	O	R^2	I	R
$O\circ R^2$	$O\circ R^2$	O	$O\circ R$	R	R^2	I

a) Podgrupy:
$H_1 = D_3$, $H_2 = (\{I\}, \circ)$, $H_3 = (\{I, O\}, \circ)$, $H_4 = (\{I, O\circ R\}, \circ)$, $H_5 = (\{I, O\circ R^2\}, \circ)$, $H_6 = (\{I, R, R^2\}, \circ)$.

b) Normální podgrupy:
$H_1 \trianglelefteq D_3$, $H_2 \trianglelefteq D_3$ (triviální podgrupy), $H_6 \trianglelefteq D_3$ (neboť $[D_3 : H_6] = 2$).

- U podgrup H_3, H_4, H_5 zjistíme, zda se rovnají rozklady na levé a pravé třídy:
  - H_3: $R\circ H_3 = R\circ\{I, O\} = \{R, O\circ R^2\}$, $H_3\circ R = \{I, O\}\circ R = \{R, O\circ R\}$;
    $R\circ H_3 \neq H_3\circ R \Longrightarrow H_3 \ntrianglelefteq D_3$.
  - H_4: $R\circ H_4 = R\circ\{I, O\circ R\} = \{R, O\}$, $H_4\circ R = \{I, O\circ R\}\circ R = \{R, O\circ R^2\}$;
    $R\circ H_4 \neq H_4\circ R \Longrightarrow H_4 \ntrianglelefteq D_3$.
  - H_5: $R\circ H_5 = R\circ\{I, O\circ R^2\} = \{R, O\circ R\}$, $H_5\circ R = \{I, O\circ R^2\}\circ R = \{R, O\circ R^3\}$;
    $R\circ H_5 \neq H_5\circ R \Longrightarrow H_5 \ntrianglelefteq D_3$.
- Můžeme řešit také tím, že ověříme, zda platí:
  $(\forall X \in D_3)\ (\forall Y \in H_i)\ \ X \circ Y \circ X^{-1} \in H_i$, $i = 3, 4, 5$
  - H_3: $R \circ O \circ R^2 = O\circ R \notin H_3 \Longrightarrow H_3 \ntrianglelefteq D_3$.
  - H_4: $R \circ O\circ R \circ R^2 = O\circ R^2 \notin H_4 \Longrightarrow H_4 \ntrianglelefteq D_3$.
  - H_5: $R \circ O\circ R^2 \circ R^2 = O \notin H_5 \Longrightarrow H_5 \ntrianglelefteq D_3$.

c) Faktorové grupy:
- $D_3/H_1 = D_3/D_3 = \{X\circ D_3;\ X \in D_3\} = \{D_3\}$.
- $D_3/H_2 = D_3/\{I\} = \{X\circ\{I\};\ X \in D_3\} = \{\{X\};\ X \in D_3\}$.
- $D_3/H_6 = \{H_6, D_3 - H_6\} = \{\{I, R, R^2\}, \{O, O\circ R, O\circ R^2\}\}$.

Příklad 6. 1. 4:
Zjistěte, zda D_4 je podgrupou grupy D_8. V kladném případě určete, zda je normální podgrupou.

Řešení:
$D_8 = (\{I, R, R^2, R^3, R^4, R^5, R^6, R^7, O, O\circ R, O\circ R^2, O\circ R^3, O\circ R^4, O\circ R^5, O\circ R^6, O\circ R^7\}, \circ)$, kde R je rotace o úhel 45°. U grupy D_4 je R rotací o úhel 90°. To znamená, že rotace R v grupě D_4 odpovídá rotaci R^2 v grupě D_8.
Takže $D_4 = (\{I, R^2, R^4, R^6, O, O\circ R^2, O\circ R^4, O\circ R^6\}, \circ)$, kde R je rotace o úhel 45°, a je tedy podgrupou grupy D_8.
Protože $|D_8| = 16$, $|D_4| = 8$, je $[D_8 : D_4] = 2$, takže $D_4 \trianglelefteq D_8$ (viz věta 4. 11.).

Příklad 6. 1. 5(∗):
Nechť $\mathbb{L}_4$, $\mathbb{L}_6$, $\mathbb{L}_8$, $\mathbb{L}_{12}$ a $\mathbb{L}_{20}$ jsou grupy symetrií pravidelných mnohostěnů. Určete jejich řád.

Řešení:
Uvažujme nejprve dvanáctistěn, který má dvanáct pětiúhelníkových stěn. Symetrie musí zobrazit zvolenou stěnu na jednu z dvanácti stěn a může tento pětiúhelník otočit či zrcadlit celkem $2\cdot5 = 10$ způsoby (jako řád D_5). $\mathbb{L}_{12}$ má tedy podle pravidla součinu stodvacet prvků, tj. $|\mathbb{L}_{12}| = 120$.
Analogicky zjistíme řády dalších grup:

- $\mathbb{L}_{20}$ má $20\cdot2\cdot3 = 120$ prvků, tj. $|\mathbb{L}_{20}| = 120$.
- $\mathbb{L}_8$ má $8\cdot2\cdot3 = 48$ prvků, tj. $|\mathbb{L}_8| = 48$; $\mathbb{L}_6$ má $6\cdot2\cdot4 = 48$ prvků, tj. $|\mathbb{L}_6| = 48$.
- $\mathbb{L}_4$ má $4\cdot2\cdot3 = 24$ prvků, tj. $|\mathbb{L}_4| = 24$.

Poznámka:
Grupy $\mathbb{L}_{12}$ a $\mathbb{L}_{20}$ jsou izomorfní, jelikož každý vrchol dvanáctistěnu lze ztotožnit se stěnou dvacetistěnu (a naopak). Totéž platí pro krychli a osmistěn, tj. $\mathbb{L}_6 \cong \mathbb{L}_8$.

Příklad 6. 1. 6(∗):
Dokažte, že grupa otočení pravidelného čtyřstěnu je izomorfní grupě A_4.

Řešení:
Označme si vrcholy pravidelného čtyřstěnu čísly 1, 2, 3, 4. Každé jeho otočení pak můžeme reprezentovat jako permutaci čísel jeho vrcholů. Každé otočení je jednoznačně určeno polohou jedné ze čtyř stěn (čtyři možnosti) a jednoho ze tří vrcholů této stěny (tři možnosti). Podle pravidla součinu tedy existuje celkem dvanáct otočení pravidelného čtyřstěnu. Osm z těchto otočení je podle osy procházející vrcholem a těžištěm protilehlé stěny (tj. rotace o 120° a 240°). Tato otočení jsou reprezentována trojcykly (vrchol, jímž prochází osa, zůstává na místě). Tři otočení jsou podle os procházejících středy protilehlých hran (tj. rotace o 180°), ta jsou reprezentována součinem dvojic transpozic. Poslední otočení je identita. Všechny tyto permutace jsou sudé a jejich počet je roven počtu sudých permutací na čtyřprvkové množině. Skládání otočení odpovídá skládání permutací. Tím je tvrzení dokázáno.

3. 6. 2. Příklady k procvičení

Příklad 6. 2. 1:
Sestavte Cayleyho tabulku pro grupu symetrií kosočtverce a rozhodněte, zda je tato grupa komutativní.

Příklad 6. 2. 2:
a) Nalezněte všechny podgrupy grupy D_4.
b) Určete, které z nich jsou normální.
c) Určete faktorové grupy podle těchto normálních podgrup.

3. 7. Homomorfismy grup

3. 7. 1. Řešené příklady

Příklad 7. 1. 1:
Rozhodněte, zda následující zobrazení jsou homomorfismy, resp. izomorfismy grup. V kladném případě určete *Ker* φ homomorfismu φ.

a) $\varphi\colon (\mathbb{R}, +) \longrightarrow (\mathbb{R}, +)$, $(\forall\, a \in \mathbb{R})\ \varphi(a) = a - 1$;
b) $\varphi\colon (\mathbb{R}^3, +) \longrightarrow (\mathbb{R}^2, +)$, $(\forall\, (x_1, x_2, x_3) \in \mathbb{R}^3)\ \varphi((x_1, x_2, x_3)) = (x_1 - x_2, x_2 - 2x_3)$;
c) $\varphi\colon (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, *)$, $(\forall\, a \in \mathbb{Z})\ \varphi(a) = a + 2$, kde operace „$*$“ je definována takto: $(\forall\, a, b \in \mathbb{Z})\ a * b = a + b - 2$;
d) $\varphi\colon (G \times H, \triangle) \longrightarrow (G, *)$, $(\forall\, (x, y) \in G \times H)\ \varphi((x, y)) = x$, kde $(G, *)$, $(H, \circ)$ jsou grupy a $(G \times H, \triangle)$ jejich direktní součin.

Řešení:
Nejprve vždy zapíšeme podmínku, která musí platit, aby dané zobrazení bylo homomorfismus.

a) $(\forall\, a, b \in \mathbb{R})\ \varphi(a + b) = \varphi(a) + \varphi(b)$
L $= \varphi(a + b) = a + b - 1$
P $= \varphi(a) + \varphi(b) = a - 1 + b - 1 = a + b - 2$
L $\neq$ P, tj. φ není homomorfismus.

b) $(\forall\, (x_1, x_2, x_3), (y_1, y_2, y_3) \in \mathbb{R}^3)$
$\varphi((x_1, x_2, x_3) + (y_1, y_2, y_3)) = \varphi((x_1, x_2, x_3)) + \varphi((y_1, y_2, y_3))$
L $= \varphi((x_1, x_2, x_3) + (y_1, y_2, y_3)) = \varphi((x_1 + y_1, x_2 + y_2, x_3 + y_3)) =$
$= (x_1 + y_1 - x_2 - y_2, x_2 + y_2 - 2x_3 - 2y_3)$
P $= \varphi((x_1, x_2, x_3)) + \varphi((y_1, y_2, y_3)) = (x_1 - x_2, x_2 - 2x_3) + (y_1 - y_2, y_2 - 2y_3) =$
$= (x_1 - x_2 + y_1 - y_2, x_2 - 2x_3 + y_2 - 2y_3)$
L = P, tj. φ je homomorfismus;
Ker $\varphi = \{(x_1, x_2, x_3) \in \mathbb{R}^3;\ \varphi((x_1, x_2, x_3)) = (0, 0)\} =$
$= \{(x_1, x_2, x_3) \in \mathbb{R}^3;\ (x_1 - x_2, x_2 - 2x_3) = (0, 0)\}$
- $x_1 - x_2 = 0 \wedge x_2 - 2x_3 = 0 \Longrightarrow x_1 = x_2 = 2x_3$;
Ker $\varphi = \{(2t, 2t, t);\ t \in \mathbb{R}\}$; φ není izomorfismus, neboť *Ker* φ není jednoprvková množina.

c) $(\forall\, a, b \in \mathbb{Z})\ \varphi(a + b) = \varphi(a) * \varphi(b)$
L $= \varphi(a + b) = a + b + 2$
P $= \varphi(a) * \varphi(b) = (a + 2) * (b + 2) = a + 2 + b + 2 - 2 = a + b + 2$
L = P, tj. φ je homomorfismus;
Určíme neutrální prvek grupy $(\mathbb{Z}, *)$:
$(\exists\, e \in \mathbb{Z})\ (\forall\, a \in \mathbb{Z})\ a * e = a$
$a + e - 2 = a$, tj. $e = 2$
Ker $\varphi = \{a \in \mathbb{Z};\ \varphi(a) = 2\} = \{a \in \mathbb{Z};\ a + 2 = 2\} = \{a \in \mathbb{Z};\ a = 0\} = \{0\}$.
Protože *Ker* φ je jednoprvková množina a φ je surjekce, je φ izomorfismus.
Poznámka: Využili jsme větu 7. 1.

d) $(\forall\, (x_1, y_1), (x_2, y_2) \in G \times H)\ \varphi((x_1, y_1) \triangle (x_2, y_2)) = \varphi((x_1, y_1)) * \varphi((x_2, y_2))$
$\varphi((x_1, y_1) \triangle (x_2, y_2)) = \varphi((x_1 * x_2, y_1 \circ y_2)) = x_1 * x_2 = \varphi((x_1, y_1)) * \varphi((x_2, y_2))$, tedy φ je homomorfismus;
Ker $\varphi = \{(x, y) \in G \times H;\ \varphi((x, y)) = e_G\} = \{(x, y) \in G \times H;\ x = e_G\} =$
$= \{(e_G, y) \in G \times H;\ y \in H\}$; tj. φ není obecně izomorfismus.

Příklad 7. 1. 2(∗)**:**

a) Dokažte, že grupa $(\{1, -1\}, \cdot)$ je homomorfním obrazem grupy $(\mathbb{R}^*, \cdot)$.

b) Dokažte, že grupa $(A, \cdot)$, kde $A = \{z \in \mathbb{K};\ |z| = 1\}$, je homomorfním, ale ne izomorfním obrazem grupy $(\mathbb{R}, +)$.

Řešení:

a) Musíme nalézt epimorfismus $\varphi: (\mathbb{R}^*, \cdot) \longrightarrow (\{1, -1\}, \cdot)$.
Definujme: $(\forall\, x \in \mathbb{R}^+)\ \ \varphi(x) = 1$,
$(\forall\, x \in \mathbb{R}^-)\ \ \varphi(x) = -1$.
Tedy φ je surjekce.

Ověříme, že φ je homomorfismus, tj. že platí: $(\forall\, x, y \in \mathbb{R}^*)\ \ \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$
- $x, y \in \mathbb{R}^+ \Longrightarrow x \cdot y \in \mathbb{R}^+ \Longrightarrow \varphi(x \cdot y) = 1 = 1 \cdot 1 = \varphi(x) \cdot \varphi(y)$,
- $x, y \in \mathbb{R}^- \Longrightarrow x \cdot y \in \mathbb{R}^+ \Longrightarrow \varphi(x \cdot y) = 1 = (-1) \cdot (-1) = \varphi(x) \cdot \varphi(y)$,
- $x \in \mathbb{R}^+, y \in \mathbb{R}^- \Longrightarrow x \cdot y \in \mathbb{R}^- \Longrightarrow \varphi(x \cdot y) = -1 = 1 \cdot (-1) = \varphi(x) \cdot \varphi(y)$,
- $x \in \mathbb{R}^-, y \in \mathbb{R}^+ \Longrightarrow x \cdot y \in \mathbb{R}^- \Longrightarrow \varphi(x \cdot y) = -1 = (-1) \cdot 1 = \varphi(x) \cdot \varphi(y)$.

Tedy grupa $(\{1, -1\}, \cdot)$ je homomorfním obrazem grupy $(\mathbb{R}^*, \cdot)$.

b) Je-li $z \in A$, pak $z = \cos x + i \cdot \sin x = e^{ix}$.
Definujme $\varphi: (\mathbb{R}, +) \longrightarrow (A, \cdot)$ předpisem: $(\forall\, x \in \mathbb{R})\ \ \varphi(x) = e^{ix}$.
Tedy φ je surjekce.
Pro každé $x, y \in \mathbb{R}$ je $\varphi(x + y) = e^{i(x+y)} = e^{ix} \cdot e^{iy} = \varphi(x) \cdot \varphi(y)$, tj. φ je homomorfismus.
Tedy grupa $(A, \cdot)$ je homomorfním obrazem grupy $(\mathbb{R}, +)$.

Ker $\varphi = \{x \in \mathbb{R};\ \varphi(x) = 1\} = \{x \in \mathbb{R};\ e^{ix} = 1\} = \{x \in \mathbb{R};\ x = 2k\pi,\ k \in \mathbb{Z}\}$.
Protože *Ker* φ je víc jak jednoprvková množina, φ není izomorfismus (není injekce).

Příklad 7. 1. 3:

Nalezněte všechny homomorfismy φ a určete *Ker* φ, jestliže:

a) $\varphi: (\mathbb{Z}_8, \oplus) \longrightarrow (\mathbb{Z}_4, \oplus)$;

b) $\varphi: (\mathbb{Z}_6, \oplus) \longrightarrow (\mathbb{Z}_7, \oplus)$;

c) $\varphi: (\mathbb{Z}_3, \oplus) \longrightarrow (\mathbb{Z}_{12}, \oplus)$.

Řešení:

a) $(\mathbb{Z}_8, \oplus) = [\overline{1}]$; určíme $\overline{y} = \varphi(\overline{1}) \in \mathbb{Z}_4$ takové, že $8 \times \overline{y} = \overline{0}$:
- $\overline{y} = \overline{0}$, tj. $\varphi_1(\overline{1}) = \overline{0} \Longrightarrow (\forall\, \overline{x} \in \mathbb{Z}_8)\ \ \varphi_1(\overline{x}) = \varphi_1(x \times \overline{1}) = x \times \varphi_1(\overline{1}) = x \times \overline{0} = \overline{0}$,
- $\overline{y} = \overline{1}$, tj. $\varphi_2(\overline{1}) = \overline{1} \Longrightarrow (\forall\, \overline{x} \in \mathbb{Z}_8)\ \ \varphi_2(\overline{x}) = \varphi_2(x \times \overline{1}) = x \times \varphi_2(\overline{1}) = x \times \overline{1} = \overline{x}$,
- $\overline{y} = \overline{2}$, tj. $\varphi_3(\overline{1}) = \overline{2} \Longrightarrow (\forall\, \overline{x} \in \mathbb{Z}_8)\ \ \varphi_3(\overline{x}) = x \times \varphi_3(\overline{1}) = x \times \overline{2} = 2 \times \overline{x}$,
- $\overline{y} = \overline{3}$, tj. $\varphi_4(\overline{1}) = \overline{3} \Longrightarrow (\forall\, \overline{x} \in \mathbb{Z}_8)\ \ \varphi_4(\overline{x}) = x \times \varphi_4(\overline{1}) = x \times \overline{3} = 3 \times \overline{x}$.
- *Ker* $\varphi_1 = \mathbb{Z}_8$;
- *Ker* φ_2: $\varphi_2(\overline{0}) = \overline{0}$, $\varphi_2(\overline{1}) = \overline{1}$, $\varphi_2(\overline{2}) = \overline{2}$, $\varphi_2(\overline{3}) = \overline{3}$, $\varphi_2(\overline{4}) = \overline{0}$, $\varphi_2(\overline{5}) = \overline{1}$,
$\varphi_2(\overline{6}) = \overline{2}$, $\varphi_2(\overline{7}) = \overline{3}$; tj. *Ker* $\varphi_2 = \{\overline{0}, \overline{4}\}$;
- *Ker* φ_3: $\varphi_3(\overline{0}) = \overline{0}$, $\varphi_3(\overline{1}) = \overline{2}$, $\varphi_3(\overline{2}) = \overline{0}$, $\varphi_3(\overline{3}) = \overline{2}$, $\varphi_3(\overline{4}) = \overline{0}$, $\varphi_3(\overline{5}) = \overline{2}$,
$\varphi_3(\overline{6}) = \overline{0}$, $\varphi_3(\overline{7}) = \overline{2}$; tj. *Ker* $\varphi_3 = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$;
- *Ker* φ_4: $\varphi_4(\overline{0}) = \overline{0}$, $\varphi_4(\overline{1}) = \overline{3}$, $\varphi_4(\overline{2}) = \overline{2}$, $\varphi_4(\overline{3}) = \overline{1}$, $\varphi_4(\overline{4}) = \overline{0}$, $\varphi_4(\overline{5}) = \overline{3}$,
$\varphi_4(\overline{6}) = \overline{2}$, $\varphi_4(\overline{7}) = \overline{1}$; tj. *Ker* $\varphi_3 = \{\overline{0}, \overline{4}\}$.

Poznámka:

Platí: $x \times \overline{k} = x \times (k \times \overline{1}) = xk \times \overline{1} = kx \times \overline{1} = k \times (x \times \overline{1}) = k \times \overline{x}$.

b) $(\mathbb{Z}_6, \oplus) = [\overline{1}]$; určíme $\overline{y} = \varphi(\overline{1}) \in \mathbb{Z}_7$ takové, že $6 \times \overline{y} = \overline{0}$:
- $\overline{y} = \overline{0}$, tj. $\varphi(\overline{1}) = \overline{0} \implies (\forall\, \overline{x} \in \mathbb{Z}_6)\ \ \varphi(\overline{x}) = x \times \overline{0} = \overline{0}$.
- *Ker* $\varphi = \mathbb{Z}_6$.

c) $(\mathbb{Z}_3, \oplus) = [\overline{1}]$; $\overline{y} = \varphi(\overline{1}) \in \mathbb{Z}_{12} \ \wedge\ 3 \times \overline{y} = \overline{0}$:
- $\overline{y} = \overline{0}$, tj. $\varphi_1(\overline{1}) = \overline{0} \implies (\forall\, \overline{x} \in \mathbb{Z}_3)\ \ \varphi_1(\overline{x}) = x \times \overline{0} = \overline{0}$,
- $\overline{y} = \overline{4}$, tj. $\varphi_2(\overline{1}) = \overline{4} \implies (\forall\, \overline{x} \in \mathbb{Z}_3)\ \ \varphi_2(\overline{x}) = x \times \overline{4} = 4 \times \overline{x}$,
- $\overline{y} = \overline{8}$, tj. $\varphi_3(\overline{1}) = \overline{8} \implies (\forall\, \overline{x} \in \mathbb{Z}_3)\ \ \varphi_3(\overline{x}) = x \times \overline{8} = 8 \times \overline{x}$.
- *Ker* $\varphi_1 = \mathbb{Z}_3$;
- *Ker* φ_2: $\varphi_2(\overline{0}) = \overline{0}$, $\varphi_2(\overline{1}) = \overline{4}$, $\varphi_2(\overline{2}) = \overline{8}$; tj. *Ker* $\varphi_2 = \{\overline{0}\}$;
- *Ker* φ_3: $\varphi_3(\overline{0}) = \overline{0}$, $\varphi_3(\overline{1}) = \overline{8}$, $\varphi_3(\overline{2}) = \overline{4}$; tj. *Ker* $\varphi_3 = \{\overline{0}\}$.

Příklad 7. 1. 4:
Nalezněte všechny homomorfismy φ: $(\mathbb{Z}, \oplus) \longrightarrow (\mathbb{Z}_5, \oplus)$.

Řešení:
$(\mathbb{Z}, +) = [1]$
- $\varphi_1(1) = \overline{0} \implies (\forall\, x \in \mathbb{Z})\ \ \varphi_1(x) = x \times \varphi_1(1) = x \times \overline{0} = \overline{0}$,
- $\varphi_2(1) = \overline{1} \implies (\forall\, x \in \mathbb{Z})\ \ \varphi_2(x) = x \times \varphi_2(1) = x \times \overline{1} = \overline{x}$,
- $\varphi_3(1) = \overline{2} \implies (\forall\, x \in \mathbb{Z})\ \ \varphi_3(x) = x \times \overline{2} = 2 \times \overline{x}$,
- $\varphi_4(1) = \overline{3} \implies (\forall\, x \in \mathbb{Z})\ \ \varphi_4(x) = x \times \overline{3} = 3 \times \overline{x}$,
- $\varphi_5(1) = \overline{4} \implies (\forall\, x \in \mathbb{Z})\ \ \varphi_5(x) = x \times \overline{4} = 4 \times \overline{x}$.

Příklad 7. 1. 5:
Dokažte:
a) *Aut* $(\mathbb{Z}_5, \oplus) \cong (\mathbb{Z}_4, \oplus)$ $(*)$;
b) *Aut* $(\mathbb{Z}_4, \oplus) \cong (\mathbb{Z}_2, \oplus)$.

Řešení:
Automorfismů existuje právě tolik, kolik má daná cyklická grupa generátorů; obrazem generátoru je opět generátor.

a) $(\mathbb{Z}_5, \oplus) = [\overline{1}] = [\overline{2}] = [\overline{3}] = [\overline{4}]$
- $\varphi_1(\overline{1}) = \overline{1} \implies (\forall\, \overline{x} \in \mathbb{Z}_5)\ \ \varphi_1(\overline{x}) = x \times \varphi_1(\overline{1}) = x \times \overline{1} = \overline{x}$,
- $\varphi_2(\overline{1}) = \overline{2} \implies (\forall\, \overline{x} \in \mathbb{Z}_5)\ \ \varphi_2(\overline{x}) = x \times \varphi_2(\overline{1}) = x \times \overline{2} = 2 \times \overline{x}$,
- $\varphi_3(\overline{1}) = \overline{3} \implies (\forall\, \overline{x} \in \mathbb{Z}_5)\ \ \varphi_3(\overline{x}) = x \times \varphi_3(\overline{1}) = x \times \overline{3} = 3 \times \overline{x}$,
- $\varphi_4(\overline{1}) = \overline{4} \implies (\forall\, \overline{x} \in \mathbb{Z}_5)\ \ \varphi_4(\overline{x}) = x \times \varphi_4(\overline{1}) = x \times \overline{4} = 4 \times \overline{x}$.

Tedy *Aut* $(\mathbb{Z}_5, \oplus) = (\{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}, \circ)$.

Aby platil daný izomorfismus, musí v grupě *Aut* $(\mathbb{Z}_5, \oplus)$ existovat prvek řádu 4. Neutrálním prvkem je φ_1, tj. $o(\varphi_1) = 1$.
Zkusme φ_2:
- $\varphi_2^2 = \varphi_2 \circ \varphi_2 \implies (\forall\, \overline{x} \in \mathbb{Z}_5)\ \ (\varphi_2 \circ \varphi_2)(\overline{x}) = \varphi_2(\varphi_2(\overline{x})) = \varphi_2(2 \times \overline{x}) =$
  $= 2 \times (2 \times \overline{x}) = 4 \times \overline{x} = \varphi_4(\overline{x})$;
- $\varphi_2^3 = \varphi_4 \circ \varphi_2 \implies (\forall\, \overline{x} \in \mathbb{Z}_5)\ \ (\varphi_4 \circ \varphi_2)(\overline{x}) = \varphi_2(\varphi_4(\overline{x})) = \varphi_2(4 \times \overline{x}) =$
  $= 2 \times (4 \times \overline{x}) = 3 \times \overline{x} = \varphi_3(\overline{x})$;
- $\varphi_2^4 = \varphi_3 \circ \varphi_2 \implies (\forall\, \overline{x} \in \mathbb{Z}_5)\ \ (\varphi_3 \circ \varphi_2)(\overline{x}) = \varphi_2(\varphi_3(\overline{x})) = \varphi_2(3 \times \overline{x}) =$
  $= 2 \times (3 \times \overline{x}) = \overline{x} = \varphi_1(\overline{x})$.

Tedy $\varphi_2^4 = \varphi_1$, tj. $o(\varphi_2) = 4$, takže *Aut* $(\mathbb{Z}_5, \oplus) = [\varphi_2] \cong (\mathbb{Z}_4, \oplus)$.

b) $(\mathbb{Z}_4, \oplus) = [\overline{1}] = [\overline{3}]$
- $\varphi_1(\overline{1}) = \overline{1} \implies (\forall\, \overline{x} \in \mathbb{Z}_4)\ \ \varphi_1(\overline{x}) = \overline{x}$,
- $\varphi_2(\overline{1}) = \overline{3} \implies (\forall\, \overline{x} \in \mathbb{Z}_4)\ \ \varphi_2(\overline{x}) = 3 \times \overline{x}$.

Tedy $Aut\ (\mathbb{Z}_4, \oplus) = (\{\varphi_1, \varphi_2\}, \circ) \cong (\mathbb{Z}_2, \oplus)$.

Příklad 7. 1. 6:
Nalezněte automorfismus φ: $(\mathbb{Z}_{10}, \oplus) \longrightarrow (\mathbb{Z}_{10}, \oplus)$ takový, že platí:
a) $\varphi(\overline{2}) = \overline{4}$;
b) $\varphi(\overline{3}) = \overline{5}$.

Řešení:
$(\mathbb{Z}_{10}, \oplus) = [\overline{1}] = [\overline{3}] = [\overline{7}] = [\overline{9}]$
- $\varphi_1(\overline{1}) = \overline{1} \implies (\forall\, \overline{x} \in \mathbb{Z}_{10})\ \ \varphi_1(\overline{x}) = \overline{x}$,
- $\varphi_2(\overline{1}) = \overline{3} \implies (\forall\, \overline{x} \in \mathbb{Z}_{10})\ \ \varphi_2(\overline{x}) = 3 \times \overline{x}$,
- $\varphi_3(\overline{1}) = \overline{7} \implies (\forall\, \overline{x} \in \mathbb{Z}_{10})\ \ \varphi_3(\overline{x}) = 7 \times \overline{x}$,
- $\varphi_4(\overline{1}) = \overline{9} \implies (\forall\, \overline{x} \in \mathbb{Z}_{10})\ \ \varphi_4(\overline{x}) = 9 \times \overline{x}$.

a) $\varphi_1(\overline{2}) = \overline{2}$, $\varphi_2(\overline{2}) = \overline{6}$, $\varphi_3(\overline{2}) = \overline{4}$, tj. $\varphi = \varphi_3$.
b) $\varphi_1(\overline{3}) = \overline{3}$, $\varphi_2(\overline{3}) = \overline{9}$, $\varphi_3(\overline{3}) = \overline{1}$, $\varphi_4(\overline{3}) = \overline{7}$; tedy takový automorfismus, aby $\varphi(\overline{3}) = \overline{5}$, neexistuje.

Příklad 7. 1. 7:
Nechť $G = (\{X \in M_n(\mathbb{R});\ \det X \neq 0\}, \cdot)$, $H = (\{B \in M_n(\mathbb{R});\ \det B = 1 \vee \det B = -1\}, \cdot)$.
Dokažte, že platí izomorfismus: $(G/H, \cdot) \cong (\mathbb{R}^+, \cdot)$.

Řešení:
- $G/H = \{X \cdot H\}_{X \in G}$
  $X{\cdot}H = \{Y \in G;\ Y = X{\cdot}B,\ B \in H\}$;
  - $X{\cdot}H = Y{\cdot}H \iff \frac{Y}{X} \in H \iff \det\frac{Y}{X} = 1 \vee \det\frac{Y}{X} = -1 \iff$
    $\iff \frac{\det Y}{\det X} = 1 \vee \frac{\det Y}{\det X} = -1 \iff \det Y = \det X \ \vee \det Y = -\det X.$

  Tedy $X{\cdot}H = \{Y \in G;\ \det Y = \det X \ \vee \det Y = -\det X\}$.
- Definujme φ: $G/H \longrightarrow \mathbb{R}^+$ předpisem: $(\forall\, X{\cdot}H \in G/H)\ \ \varphi(X{\cdot}H) = |\det X|$.
  - Platí:
    $(\forall\, X{\cdot}H,\ Y{\cdot}H \in G/H)\ \ \varphi(X{\cdot}H \cdot Y{\cdot}H) = \varphi(X{\cdot}Y{\cdot}H) = |\det X{\cdot}Y| = |\det X \cdot \det Y| =$
    $= |\det X| \cdot |\det Y| = \varphi(X{\cdot}H) \cdot \varphi(Y{\cdot}H)$, tedy φ je homomorfismus.
  - Ke každému $X \in G$ existuje $a \in \mathbb{R}^+$ takové, že $a = |\det X|$. Zároveň ale máme $|\det X| = \varphi(X{\cdot}H)$, tj. k prvku $a \in \mathbb{R}^+$ existuje $X{\cdot}H \in G/H$ tak, že $a = \varphi(X{\cdot}H)$. To znamená, že φ je zobrazení na množinu. Protože φ je zobrazení celé množiny, je to surjekce.
  - $Ker\ \varphi = \{X{\cdot}H \in G/H;\ \varphi(X{\cdot}H) = 1\} = \{X{\cdot}H \in G/H;\ |\det X| = 1\} = \{H\}$; tedy $Ker\ \varphi$ je jednoprvková množina, tj. φ je injekce.
  - Dohromady φ je bijekce, tedy izomorfismus.

Příklad 7. 1. 8:
Nechť $(G, \cdot)$ je grupa, $\varphi: G \longrightarrow G$ zobrazení určené předpisem $\varphi(x) = x^{-1}$ pro libovolné $x \in G$. Dokažte, že φ je izomorfismus, je-li grupa $(G, \cdot)$ je komutativní.

Řešení:

- Nechť $x, y \in G$ libovolné takové, že $\varphi(x) = \varphi(y)$. Pak $x^{-1} = y^{-1}$, a tedy $x = y$. To znamená, že φ je injekce. Protože φ je zřejmě surjekce, je to dohromady bijekce.
- Dále musí platit: $(\forall\, x, y \in G)\ \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$
  $\varphi(x \cdot y) = (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ (viz věta 2. 1.),
  $\varphi(x) \cdot \varphi(y) = x^{-1} \cdot y^{-1}$.
  Je-li $(G, \cdot)$ komutativní, pak $y^{-1} \cdot x^{-1} = x^{-1} \cdot y^{-1}$, a tedy $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

Příklad 7. 1. 9$(*)$**:**
Je dán předpis $\varphi: (\mathbb{Z}_3, \oplus) \longrightarrow (S_4, \cdot)$, kde $(\forall\, \overline{x} \in \mathbb{Z}_3)\ \varphi(\overline{x}) = (1, 2)\cdot(3, 4)\cdot(1, 2, 3)^x$. Rozhodněte, zda φ korektně zadává zobrazení a zda se jedná o homomorfismus.

Řešení:
Zjistit, zda se jedná o korektně zadané zobrazení, znamená dokázat, že nezáleží na volbě reprezentantů téže zbytkové třídy. Musíme tedy zjistit, zda platí rovnost $\varphi(\overline{x}) = \varphi(\overline{x + 3k})$, kde $k \in \mathbb{Z}$. Protože (1, 2, 3) je řádu 3, máme $(1, 2)\cdot(3, 4)\cdot(1, 2, 3)^{x\,+\,3k} = (1, 2)\cdot(3, 4)\cdot(1, 2, 3)^x$. Rovnost tedy platí a předpis korektně definuje zobrazení.
Dále ověříme, zda $(\forall\, \overline{x}, \overline{y} \in \mathbb{Z}_3)\ \varphi(\overline{x} \oplus \overline{y}) = \varphi(\overline{x}) \cdot \varphi(\overline{y})$:
$L = \varphi(\overline{x} \oplus \overline{y}) = (1, 2)\cdot(3, 4)\cdot(1, 2, 3)^{x\,+\,y} = (1, 2)\cdot(3, 4)\cdot(1, 2, 3)^x \cdot(1, 2, 3)^y$
$P = \varphi(\overline{x}) \cdot \varphi(\overline{y}) = (1, 2)\cdot(3, 4)\cdot(1, 2, 3)^x \cdot(1, 2)\cdot(3, 4)\cdot(1, 2, 3)^y$.
Protože $L \neq P$, φ není homomorfismus.

3. 7. 2. Příklady k procvičení

Příklad 7. 2. 1:
Rozhodněte, zda následující zobrazení jsou homomorfismy, resp. izomorfismy grup. V kladném případě určete *Ker* φ homomorfismu φ.

a) $\varphi: (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +),\ \ (\forall\, a \in \mathbb{Z})\ \varphi(a) = 3a$;
b) $\varphi: (\mathbb{K}^*, \cdot) \longrightarrow (\mathbb{R}^*, \cdot),\ \ (\forall\, z \in \mathbb{K}^*)\ \varphi(z) = 1 + |z|$;
c) $\varphi: (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}^+, \cdot),\ \ (\forall\, a \in \mathbb{R}^+)\ \varphi(a) = \frac{1}{\sqrt{a}}$.

Příklad 7. 2. 2:
Nalezněte všechny homomorfismy φ a určete *Ker* φ, jestliže:

a) $\varphi: (\mathbb{Z}_6, \oplus) \longrightarrow (\mathbb{Z}_3, \oplus)$;
b) $\varphi: (\mathbb{Z}_3, \oplus) \longrightarrow (\mathbb{Z}_9, \oplus)$.

3. 8. Konečné grupy

Definice: Nechť p je prvočíslo. Grupy řádu p^k, kde $k \in \mathbb{Z}^+$, se nazývají p-grupy.

Věta: Nechť G je konečná abelovská grupa, $|G| > 1$. Pak $G \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_m^{k_m}}$, kde $p_1, \ldots, p_m$ jsou prvočísla a $k_1, \ldots, k_m \in \mathbb{Z}^+$. Tento rozklad grupy G na součin netriviálních cyklických p-grup je určen až na pořadí činitelů jednoznačně.

Příklad 8. 1:
Popište všechny (až na izomorfismus) komutativní grupy o 120 prvcích.

Řešení:
Číslo 120 vyjádříme jako součin mocnin prvočísel (ne nutně různých):
$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2 \cdot 2^2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$.
Dostáváme tedy tři grupy: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$, $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8$.

Příklad 8. 2:
Kolik existuje (až na izomorfismus) komutativních grup o 32 prvcích? Určete je.

Řešení:
$32 = 2^5 = 2 \cdot 2^4 = 2 \cdot 2 \cdot 2^3 = 2 \cdot 2 \cdot 2 \cdot 2^2 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^2 \cdot 2^3 = 2 \cdot 2^2 \cdot 2^2$.
Až na izomorfismus tedy existuje sedm komutativních grup o 32 prvcích:
$\mathbb{Z}_{32}$, $\mathbb{Z}_2 \times \mathbb{Z}_{16}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4$.

Následující tabulka obsahuje seznam všech (až na izomorfismus) nejvýše osmiprvkových grup a několik obecných výsledků; p značí libovolné liché prvočíslo.

n	Grupy s n prvky
1	$\mathbb{Z}_1$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$, $S_3 \cong D_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Q_8
p	$\mathbb{Z}_p$
p^2	$\mathbb{Z}_{p^2}$, $\mathbb{Z}_p \times \mathbb{Z}_p$
$2p$	$\mathbb{Z}_{2p}$, D_p

Poznámka:
Grupa Q_8 je generována dvěma prvky a, b takovými, že $o(a) = o(b) = 4$ a platí:
$a^2 = b^2$, $ab = ba^3$.
Tedy $Q_8 = [a, b; a^4 = b^4 = 1, a^2 = b^2, ab = ba^3] = (\{1, a, a^2, a^3, b, ba, ba^2, ba^3\}, \cdot)$. Tato grupa se nazývá kvaternionová grupa.

Příklad 8. 3(∗):
Zkonstruujte multiplikativní grupu P, která je generována prvky io^x, io^y, io^z, kde $i^2 = -1$, $(o^x)^2 = (o^y)^2 = (o^z)^2 = 1$, $o^x o^y = io^z = -o^y o^x$ (v posledním vztahu lze cyklicky zaměňovat indexy, aniž by to mělo vliv na jeho platnost).
Dále nalezněte řád této grupy, třídy konjugovaných prvků a jejich řády. Srovnejte s grupou D_4 symetrií čtverce a ukažte, že nejsou izomorfní navzdory stejnému řádu grupy.

Poznámka:
Chápejme io^x, io^y, io^z jako abstraktní algebraické objekty, o kterých víme jen to, že pro ně platí vztahy uvedené v zadání.

Řešení:
Kromě jednotkového prvku 1 a generátorů musíme do grupy zahrnout také $(io^x)^2 = -1$ a inverzní prvky ke generátorům, tj. prvky $(io^j)^{-1} = -io^j$, kde $j = x, y, z$.
Tedy $P = (\{\pm 1, \pm io^x, \pm io^y, \pm io^z\}, \cdot)$, proto $|P| = 8$.
Skutečně jde o grupu:

- P je uzavřená vzhledem k násobení (např. $io^x \cdot io^y = -io^z$, analogicky se ověří všechny možné součiny prvků z P);
- P obsahuje jednotkový prvek a ke každému prvku prvek inverzní;
- násobení je asociativní.

Třídy konjugovaných prvků, řády prvků:

- Jednotkový prvek má vždy svou vlastní třídu, $o(1) = 1$.
- Prvek -1 má také svoji třídu, protože i ten komutuje se všemi prvky grupy, $o(-1) = 2$, neboť $(-1)^2 = 1$.
- Lze ověřit, že pro všechna $g, h \in P$ je $g^{-1}hg = h$ (resp. $-h$), tudíž io^x a io^y nemohou být konjugované. Naopak $io^x \sim -io^x$ (a podobně y, z), jelikož např.:
  $(io^y)^{-1}(io^x)(io^y) = (io^y)^{-1}(-io^z) = (-io^y)(-io^z) = -o^y o^z = -io^x$.
  Dostáváme tedy pět různých tříd: $\{\{1\}, \{-1\}, \{io^x, -io^x\}, \{io^y, -io^y\}, \{io^z, -io^z\}\}$.

Řád každého z šesti prvků $(\pm io^j)$ je roven 4, zatímco grupa D_4 má jen dva prvky řádu 4 (rotace R (o úhel 90°) a rotace R^3 (o úhel 270°)). Tedy tyto grupy nemohou být izomorfní.

Příklad 8. 4:
Jsou dány grupy $G = (\mathbb{Z}_2 \times \mathbb{Z}_8, \oplus)$ a $H = [a, x; a^2 = x^8 = 1, ax = x^5 a]$. Ukažte, že ačkoli mají stejný počet prvků každého řádu, nejsou izomorfní.

Řešení:
$G = (\mathbb{Z}_2 \times \mathbb{Z}_8, \oplus) = (\{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{0}, \overline{3}), (\overline{0}, \overline{4}), (\overline{0}, \overline{5}), (\overline{0}, \overline{6}), (\overline{0}, \overline{7}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2}), (\overline{1}, \overline{3}), (\overline{1}, \overline{4}), (\overline{1}, \overline{5}), (\overline{1}, \overline{6}), (\overline{1}, \overline{7})\}, \oplus)$.

Řády prvků grupy G:

- $(\overline{0}, \overline{0})$…řád 1;
- $(\overline{0}, \overline{4})$, $(\overline{1}, \overline{0})$, $(\overline{1}, \overline{4})$…řád 2;
- $(\overline{0}, \overline{2})$, $(\overline{0}, \overline{6})$, $(\overline{1}, \overline{2})$, $(\overline{1}, \overline{6})$…řád 4;
- $(\overline{0}, \overline{1})$, $(\overline{0}, \overline{3})$, $(\overline{0}, \overline{5})$, $(\overline{0}, \overline{7})$, $(\overline{1}, \overline{1})$, $(\overline{1}, \overline{3})$, $(\overline{1}, \overline{5})$, $(\overline{1}, \overline{7})$…řád 8.

Tedy G má jeden prvek řádu 1, tři prvky řádu 2, čtyři prvky řádu 4 a osm prvků řádu 8.

$H = (\{1, x, x^2, x^3, x^4, x^5, x^6, x^7, xa, x^2a, x^3a, x^4a, x^5a, x^6a, x^7a, a\}, \cdot)$

Pro grupu H sestavíme Cayleyho tabulku, ze které určíme řády všech jejích prvků.
K sestavení tabulky použijeme definující relace této grupy, tj. např. máme:
$xa \cdot x^3 = x \cdot ax \cdot x^2 = x \cdot x^5a \cdot x^2 = x^6 \cdot ax \cdot x = x^6 \cdot x^5a \cdot x = x^{11} \cdot ax = x^{11} \cdot x^5a = (x^8)^2a = a.$

Cayleyho tabulka:

$\cdot$	1	x	x^2	x^3	x^4	x^5	x^6	x^7	xa	x^2a	x^3a	x^4a	x^5a	x^6a	x^7a	a
1	1	x	x^2	x^3	x^4	x^5	x^6	x^7	xa	x^2a	x^3a	x^4a	x^5a	x^6a	x^7a	a
x	x	x^2	x^3	x^4	x^5	x^6	x^7	1	x^2a	x^3a	x^4a	x^5a	x^6a	x^7a	a	xa
x^2	x^2	x^3	x^4	x^5	x^6	x^7	1	x	x^3a	x^4a	x^5a	x^6a	x^7a	a	xa	x^2a
x^3	x^3	x^4	x^5	x^6	x^7	1	x	x^2	x^4a	x^5a	x^6a	x^7a	a	xa	x^2a	x^3a
x^4	x^4	x^5	x^6	x^7	1	x	x^2	x^3	x^5a	x^6a	x^7a	a	xa	x^2a	x^3a	x^4a
x^5	x^5	x^6	x^7	1	x	x^2	x^3	x^4	x^6a	x^7a	a	xa	x^2a	x^3a	x^4a	x^5a
x^6	x^6	x^7	1	x	x^2	x^3	x^4	x^5	x^7a	a	xa	x^2a	x^3a	x^4a	x^5a	x^6a
x^7	x^7	1	x	x^2	x^3	x^4	x^5	x^6	a	xa	x^2a	x^3a	x^4a	x^5a	x^6a	x^7a
xa	xa	x^6a	x^3a	a	x^5a	x^2a	x^7a	x^4a	x^6	x^3	1	x^5	x^2	x^7	x^4	x
x^2a	x^2a	x^7a	x^4a	xa	x^6a	x^3a	a	x^5a	x^7	x^4	x	x^6	x^3	1	x^5	x^2
x^3a	x^3a	a	x^5a	x^2a	x^7a	x^4a	xa	x^6a	1	x^5	x^2	x^7	x^4	x	x^6	x^3
x^4a	x^4a	xa	x^6a	x^3a	a	x^5a	x^2a	x^7a	x	x^6	x^3	1	x^5	x^2	x^7	x^4
x^5a	x^5a	x^2a	x^7a	x^4a	xa	x^6a	x^3a	a	x^2	x^7	x^4	x	x^6	x^3	1	x^5
x^6a	x^6a	x^3a	a	x^5a	x^2a	x^7a	x^4a	xa	x^3	1	x^5	x^2	x^7	x^4	x	x^6
x^7a	x^7a	x^4a	xa	x^6a	x^3a	a	x^5a	x^2a	x^4	x	x^6	x^3	1	x^5	x^2	x^7
a	a	x^5a	x^2a	x^7a	x^4a	xa	x^6a	x^3a	x^5	x^2	x^7	x^4	x	x^6	x^3	1

Řády prvků grupy H:

- 1…řád 1;
- a, x^4, x^4a…řád 2;
- x^2, x^6, x^2a, x^6a…řád 4;
- $x, x^3, x^5, x^7, xa, x^3a, x^5a, x^7a$…řád 8.

Tedy H má také jeden prvek řádu 1, tři prvky řádu 2, čtyři prvky řádu 4 a osm prvků řádu 8.

Z Cayleyho tabulky je zřejmé, že H není komutativní; nemůže být proto izomorfní s komutativní grupou G.

3. 9. Výsledky příkladů

3. 9. 1. Algebraické struktury s jednou operací

Příklad 1. 2. 1:
a) Ano, b) ne, c) ano, d) ne.

Příklad 1. 2. 2:
$x = 0{,}28$

Příklad 1. 2. 3:
$(G, \circ)$ je komutativní, není asociativní, má neutrální prvek d.

Příklad 1. 2. 4:
a) Je komutativní, není asociativní, neutrální prvek je 0.
b) Není komutativní, je asociativní, nemá neutrální prvek.

Příklad 1. 2. 5:
a) Neutrálním prvkem je 0; inverzním prvkem k 0 (resp. 2) je 0 (resp. 2), k ostatním prvkům inverzní prvky neexistují.
b) Neutrálním prvkem je $\overline{1}$; inverzním prvkem k $\overline{1}$ (resp. $\overline{5}$) je $\overline{1}$ (resp. $\overline{5}$), k ostatním prvkům inverzní prvky neexistují.

Příklad 1. 2. 6:
a) Grupoid s neutrálním prvkem 1 a s krácením.
b) Komutativní kvazigrupa.
c) Komutativní kvazigrupa.
d) Komutativní pologrupa s neutrálním prvkem $\emptyset$ (komutativní monoid) a s agresivním prvkem A.

Příklad 1. 2. 7:
a) Grupoid s neutrálním prvkem a.
b) Komutativní grupoid s neutrálním prvkem c a s agresivním prvkem a.

Příklad 1. 2. 8:
Podgrupoidy: $(\{a\}, \cdot)$, $(\{b\}, \cdot)$, $(\{d\}, \cdot)$, $(\{b, c\}, \cdot)$, $(\{a, d\}, \cdot)$, $(\{a, b, c\}, \cdot)$, $(G, \cdot)$.
Podpologrupy: $(\{a\}, \cdot)$, $(\{b\}, \cdot)$, $(\{d\}, \cdot)$, $(\{b, c\}, \cdot)$, $(\{a, d\}, \cdot)$.
Podgrupy: $(\{a\}, \cdot)$, $(\{b\}, \cdot)$, $(\{d\}, \cdot)$, $(\{b, c\}, \cdot)$.

3. 9. 2. Základní vlastnosti grup

Příklad 2. 2. 1:
a) Ano, b) ano.

Příklad 2. 2. 2:
Ano.

Příklad 2. 2. 3:
a) Ano, komutativní grupa.
b) Ne, je to monoid (neutrálním prvkem je jednotková matice).
c) Ano, nekomutativní grupa.

Příklad 2. 2. 4:

a) Ne, $(\mathbb{N}, +)$ je komutativní monoid.
b) Ne, $(\mathbb{Q}^+, +)$ je komutativní pologrupa.
c) Ano.

Příklad 2. 2. 5:

a) Ano, b) ano.

Příklad 2. 2. 6:

Ano.

Příklad 2. 2. 7:

a) $o(\emptyset) = 1$, $o(\{1\}) = o(\{2\}) = o(\{1, 2\}) = 2$.
b) $o(\overline{0}) = 1$, $o(\overline{4}) = 2$, $o(\overline{2}) = o(\overline{6}) = 4$, $o(\overline{1}) = o(\overline{3}) = o(\overline{5}) = o(\overline{7}) = 8$.

3. 9. 3. Cyklické grupy

Příklad 3. 2. 1:

a) $(\mathbb{Z}_7, \oplus) = [\overline{1}] = [\overline{2}] = [\overline{3}] = [\overline{4}] = [\overline{5}] = [\overline{6}]$.
b) $(\mathbb{Z}_{14}, \oplus) = [\overline{1}] = [\overline{3}] = [\overline{5}] = [\overline{9}] = [\overline{11}] = [\overline{13}]$.
c) $(\mathbb{Z}_{20}, \oplus) = [\overline{1}] = [\overline{3}] = [\overline{7}] = [\overline{9}] = [\overline{11}] = [\overline{13}] = [\overline{17}] = [\overline{19}]$.

Příklad 3. 2. 2:

a) $H_1 = (\mathbb{Z}_5, \oplus)$, $H_2 = (\{\overline{0}\}, \oplus)$.
b) $H_1 = (\mathbb{Z}_{30}, \oplus)$, $H_2 = (\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \ldots, \overline{28}\}, \oplus)$, $H_3 = (\{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \ldots, \overline{27}\}, \oplus)$, $H_4 = (\{\overline{0}, \overline{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}\}, \oplus)$, $H_5 = (\{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}\}, \oplus)$, $H_6 = (\{\overline{0}, \overline{10}, \overline{20}\}, \oplus)$, $H_7 = (\{\overline{0}, \overline{15}\}, \oplus)$, $H_8 = (\{\overline{0}\}, \oplus)$.

Příklad 3. 2. 3:

$(\mathbb{Z}_{11}^*, \odot) = [\overline{2}] = [\overline{6}] = [\overline{7}] = [\overline{8}]$.
Podgrupy: $H_1 = (\mathbb{Z}_{11}^*, \odot)$, $H_2 = (\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}, \odot)$, $H_3 = (\{\overline{1}, \overline{10}\}, \odot)$, $H_4 = (\{\overline{1}\}, \odot)$.

Příklad 3. 2. 4:

$(A, \odot)$:

- není cyklická (všechny prvky kromě neutrálního jsou řádu 2);
- podgrupy: $H_1 = (A, \odot)$, $H_2 = (\{\overline{1}, \overline{3}\}, \odot)$, $H_3 = (\{\overline{1}, \overline{5}\}, \odot)$, $H_4 = (\{\overline{1}, \overline{7}\}, \odot)$, $H_5 = (\{\overline{1}\}, \odot)$.

$(B, \odot)$:

- je cyklická, $(B, \odot) = [\overline{2}] = [\overline{5}]$;
- podgrupy: $H_1 = (B, \odot)$, $H_2 = (\{\overline{1}, \overline{4}, \overline{7}\}, \odot)$, $H_3 = (\{\overline{1}, \overline{8}\}, \odot)$, $H_4 = (\{\overline{1}\}, \odot)$.

Příklad 3. 2. 5:

- $(\mathbb{Z}_6 \times \mathbb{Z}_7, \oplus) = [(\overline{1}, \overline{1})] = [(\overline{1}, \overline{2})] = [(\overline{1}, \overline{3})] = [(\overline{1}, \overline{4})] = [(\overline{1}, \overline{5})] = [(\overline{1}, \overline{6})] =$
  $= [(\overline{5}, \overline{1})] = [(\overline{5}, \overline{2})] = [(\overline{5}, \overline{3})] = [(\overline{5}, \overline{4})] = [(\overline{5}, \overline{5})] = [(\overline{6}, \overline{6})]$;
- $(\mathbb{Z}_5 \times \mathbb{Z}_{10}, \oplus)$ není cyklická grupa.

3. 9. 4. Rozklady podle podgrupy

Příklad 4. 2. 1:
$G/H = \mathbb{R} / \mathbb{Z} = \{x + \mathbb{Z}\}_{x \in \mathbb{R}}$; $x + \mathbb{Z} = \{y \in \mathbb{R}; y - x \in \mathbb{Z}\}$.

Příklad 4. 2. 2:
a) $G/H = \{\{\overline{0}, \overline{4}\}, \{\overline{1}, \overline{5}\}, \{\overline{2}, \overline{6}\}, \{\overline{3}, \overline{7}\}\}$.
b) $G/H = \{0 + [2], 1 + [2]\}$.

Příklad 4. 2. 3:
$H \trianglelefteq G$.

3. 9. 5. Permutační grupy

Příklad 5. 2. 1:
a) $\Pi = (1, 6)\cdot(2, 7, 4)\cdot(3, 5)$, $o(\Pi) = 6$, sudá, $\Pi^{-1} = (1, 6)\cdot(4, 7, 2)\cdot(3, 5)$.
b) $\Pi = (1, 4, 3)\cdot(2, 8, 6, 7)$, $o(\Pi) = 12$, lichá, $\Pi^{-1} = (3, 4, 1)\cdot(7, 6, 8, 2)$.

Příklad 5. 2. 2:
a) $\Pi^{68} = (3, 4, 6)$; b) $\Pi^{136} = (3, 6, 4)$; c) $\Pi^{1212} = I$.

Příklad 5. 2. 3:
a) $A = (1, 2, 3)\cdot(4, 5)$, $B = (1, 4, 3, 2)$.
b) $A \cdot B = (3, 4, 5)$.
c) $A^{15} = (4, 5)$.
d) $B = (1, 2)\cdot(1, 3)\cdot(1, 4)$.

Příklad 5. 2. 4:
a) $A = (1, 9, 5)\cdot(2, 3, 7)\cdot(4, 8, 6)$, $B = (1, 8, 4, 2)\cdot(3, 5, 6)$, $C = (1, 9, 6, 2, 5, 8, 3, 7)$.
b) A je sudá, B je lichá, C je lichá.
c) $D = (1, 9, 6, 4, 8, 3, 7, 2, 5)$.

Příklad 5. 2. 5:
Sudá.

Příklad 5. 2. 6:
Ne.

3. 9. 6. Grupy symetrií

Příklad 6. 2. 1:
Viz příklad 6. 1. 1. (grupa symetrií kosočtverce je izomorfní s grupou symetrií obdélníku).

Příklad 6. 2. 2:
a) $H_1 = D_4$, $H_2 = (\{I\}, \circ)$, $H_3 = (\{I, R, R^2, R^3\}, \circ)$, $H_4 = (\{I, O\}, \circ)$, $H_5 = (\{I, O\circ R\}, \circ)$, $H_6 = (\{I, O\circ R^2\}, \circ)$, $H_7 = (\{I, O\circ R^3\}, \circ)$, $H_8 = (\{I, R^2\}, \circ)$, $H_9 = (\{I, R^2, O, O\circ R^2\}, \circ)$, $H_{10} = (\{I, R^2, O\circ R, O\circ R^3\}, \circ)$.
b) H_1, H_2, H_3, H_8, H_9, H_{10}.
c) $D_4/H_1 = \{D_4\}$, $D_4/H_2 = \{\{X\}; X \in D_4\}$, $D_4/H_3 = \{H_3, D_4 - H_3\}$, $D_4/H_8 = \{\{I, R^2\}, \{R, R^3\}, \{O, O\circ R^2\}, \{O\circ R, O\circ R^3\}\}$, $D_4/H_9 = \{H_9, D_4 - H_9\}$, $D_4/H_{10} = \{H_{10}, D_4 - H_{10}\}$.

3. 9. 7. Homomorfismy grup

Příklad 7. 2. 1:

a) φ je homomorfismus, ale není izomorfismus (není surjekce), $Ker\ \varphi = \{0\}$;
b) φ není homomorfismus;
c) φ je izomorfismus, $Ker\ \varphi = \{1\}$.

Příklad 7. 2. 2:

a) $(\forall\ \overline{x} \in \mathbb{Z}_6)$ $\varphi_1(\overline{x}) = \overline{0}$, $\varphi_2(\overline{x}) = \overline{x}$, $\varphi_3(\overline{x}) = 2 \times \overline{x}$;
$Ker\ \varphi_1 = \mathbb{Z}_6$, $Ker\ \varphi_2 = Ker\ \varphi_3 = \{\overline{0}, \overline{3}\}$.

b) $(\forall\ \overline{x} \in \mathbb{Z}_3)$ $\varphi_1(\overline{x}) = \overline{0}$, $\varphi_2(\overline{x}) = 3 \times \overline{x}$, $\varphi_3(\overline{x}) = 6 \times \overline{x}$;
$Ker\ \varphi_1 = \mathbb{Z}_3$, $Ker\ \varphi_2 = Ker\ \varphi_3 = \{\overline{0}\}$.

4. Literatura

[1] BLAŽEK, Jaroslav, et al. *Algebra a teoretická aritmetika I. díl*. 1. vydání. Praha : SPN, 1983. 278 s.

[2] BLAŽEK, Jaroslav; KOMAN, Milan; VOJTÁŠKOVÁ, Blanka. *Algebra a teoretická aritmetika II. díl*. 1. vydání. Praha : SPN, 1985. 258 s.

[3] FADDEJEV, A. K.; SOMINSKIJ, J. S. *Zbierka úloh z vyššej algebry*. Bratislava : Alfa, 1968.

[4] HORÁK, Pavel. *Cvičení z algebry a teoretické aritmetiky*. Brno : MU, 2002.

[5] CHAJDA, Ivan. *Vybrané kapitoly z algebry*. 2. vydání. Olomouc : Univerzita Palackého v Olomouci, 2000.

[6] MAC LANE, S.; BIRKHOFF, G. *Algebra*. Bratislava : Alfa, 1967. 662 s.

[7] PROCHÁZKA, Ladislav, et al. *Algebra*. 1. vydání. Praha : Academia, 1990.

[8] HORÁKOVÁ, Lucie. *Grupy symetrií* [online]. Brno : Masarykova Univerzita, 2006. 66 s. Bakalářská práce. Masarykova Univerzita, Přírodovědecká fakulta. [cit. 2010-07-27]. Dostupné z WWW: <http://is.muni.cz/th/106253/prif_b/Grupy_symetrii.pdf>.

[9] MUSIL, Vít. *Grupy : Sbírka příkladů* [online]. Brno : Masarykova Univerzita, 2005. 48 s. Bakalářská práce. Masarykova Univerzita, Přírodovědecká fakulta. [cit. 2010-07-27]. Dostupné z WWW: <http://www.math.muni.cz/~klima/Algebra/grupy_sbirka.pdf>.

[10] STANOVSKÝ, David. *Příklady z algebry* [online]. Praha : Univerzita Karlova [cit. 2010-07-27].
Dostupné z WWW: <http://www.karlin.mff.cuni.cz/~stanovsk/vyuka/sbirka.pdf>.