Západočeská univerzita v Plzni

FAKULTA PEDAGOGICKÁ

BAKALÁŘSKÁ PRÁCE

KONEČNÉ GRUPY MALÝCH ŘÁDŮ

Ivana Čechová

Vedoucí práce: *doc. RNDr. Jaroslav Hora, CSc.*

Plzeň 2012

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 21. března 2012

……
podpis

Touto cestou bych chtěla velmi poděkovat mému vedoucímu bakalářské práce **doc. RNDr. Jaroslavu Horovi, CSc.**, za odborné vedení, pomoc a cenné rady v průběhu jejího zpracování.

Obsah

Úvod

Pro svoji bakalářskou práci jsem si zvolila téma s názvem: „Konečné grupy malých řádů“. Toto téma se zabývá především problematikou komutativních a nekomutativních grup a jejich vlastnostmi. Grupy jsou označeny číselnými řády, jenž určují počet prvků v grupě. Studiem grup se zabývá matematická disciplína s názvem teorie grup, za jehož představitele je považován francouzský matematik Évariste Galois.

Tato práce je rozdělena na šest kapitol, v nichž se mimo teoretických textů vyskytují také názorné ukázky v podobě různých příkladů.

První kapitola se zabývá binárními algebraickými operacemi a jejich vlastnostmi, které budou nadále potřebné pro další studium grup.

Na toto téma hned navazuje druhá kapitola, ve které budu definovat jednotlivé pojmy algebraických struktur spojené s ukázkami. Ve druhé polovině této kapitoly již uvedu čtenáře do problematiky konečných grup malých řádů a sjednotím některá značení, která budu používat po zbytek práce.

Třetí kapitola se zabývá homomorfizmem a izomorfizmem, což jsou zvláštní druhy zobrazení jedné algebraické struktury do jiné, které si zachovávají určité vlastnosti. Nadefinuji jednotlivé pojmy, uvedu věty spojené s tímto tématem a připojím příklady.

Ve čtvrté kapitole již budu studovat konečné grupy řádu 4 a konečné grupy řádu 6. Ukáži postup hledání řešení pro zpracování operačních tabulek a způsob jak pomocí grup s tzv. nižším řádem zkonstruovat grupy s tzv. vyšším řádem.

Pátá kapitola pojednává o komutativních grupách a dále o zpracovávání operačních tabulek komutativních grup s neprvočíselnými řády.

V poslední šesté kapitole se zaměřím na nekomutativní grupy řádu 8 až řádu 15, kde k nim budu také zpracovávat operační tabulky.

1 Binární algebraické operace

V této kapitole shrneme a zopakujeme binární algebraické operace, na které dále navazují základní algebraické struktury a jejich vlastnosti.

1.1 Binární operace na množině

Pojem binární algebraické operace otevírá cestu k definici některých základních algebraických struktur. V libovolné neprázdné množině A budeme binární algebraickou operaci chápat jako předpis, který přiřazuje uspořádané dvojici (a, b) $\in$ A x A právě jeden prvek c $\in$ A. Prvek c je potom výsledkem operace s prvky a, b v takto udávaném pořadí. [1]

Definice 1 Binární operace

Binární operací v libovolné neprázdné množině A rozumíme každé zobrazení

ω: A x A $\rightarrow$ A. Jestliže v operaci ω přísluší uspořádané dvojici (a, b) $\in$ A x A jako obraz prvek c $\in$ A, pak místo obvyklého zápisu

c = (a, b) ω

píšeme

c = a ω b

a říkáme, že prvek c je výsledkem operace ω s prvky a a b v tomto pořadí. [1]

Například můžeme uvést:

$$[3;3] \xrightarrow{+} 6$$

tedy:

$$3 + 3 = 6.$$ [4]

Nejčastějšími binárními algebraickými operacemi jsou námi známé aritmetické operace sčítání a násobení. Tyto operace můžeme provádět na množinách čísel přirozených, celých, racionálních, komplexních. Oproti tomu aritmetické operace odčítání lze provádět pouze na množinách čísel celých, racionálních či komplexních. Na množině čísel přirozených nelze provést aritmetickou operaci odčítání, neboť nemůžeme ke každé uspořádané dvojici (a, b) přiřadit libovolné číslo c $\in$ N takové, aby platilo c = a – b.

V definici 1 jsme binární algebraickou operaci nazvali symbolem ω. Avšak místo tohoto symbolu se užívají především znaky +, *, -, /, $\cap$, $\cup$ atd. Potom již můžeme binární algebraickou operaci * zapisovat ve tvaru c = a * b. [1]

1.2 Vlastnosti binárních algebraických operací

Nyní se budeme zabývat vlastnostmi binárních algebraických operací. Bez těchto vlastností je totiž pojem binární algebraické operace na množině příliš obecným pojmem. [1]

Definice 2 Komutativní binární algebraická operace

Binární algebraická operace * definovaná na množině $A \neq \emptyset$ se nazývá komutativní, právě když

$\forall$ a, b $\in$ A; a * b = b * a.

Tato rovnost se nazývá komutativní zákon. [1]

Příklad 1

Jako příklad komutativních operací lze uvést číselné operace sčítání, násobení, množinové operace sjednocení a průnik, logické operace konjunkce či disjunkce.

Také operace * definovaná předpisem

a * b = 2a +2b; a, b $\in$ C

pro níž

a * b = 2a +2b = 2b +2a = b * a, je komutativní.

Mezi nekomutativní binární operace řadíme operace odčítání a dělení. [4]

Definice 3 Asociativní binární algebraická operace

Binární algebraická operace * definovaná na množině $A \neq \emptyset$ se nazývá asociativní, právě když

$\forall$ a,b,c $\in$ A; (a * b) * c = a * (b * c).

Tato rovnost se nazývá asociativní zákon. [1]

Příklad 2

Za příklady asociativních binárních algebraických operací můžeme považovat ty samé, jako jsme uvedli u komutativních binárních algebraických operací.

Například binární operace:

$a * b = a + 3ab + b; a, b \in C$

$(a * b) * c = (a + 3ab + b) * c = a + b + c + 3ab + 3bc + 3ac + 9abc$

$a * (b * c) = a * (b + 3bc + c) = a + b + c + 3ab + 3bc + 3ac + 9abc$. [4]

Definice 4 Neutrální prvek

Budiž * libovolná binární algebraická operace definovaná na množině $A \neq \emptyset$. Pak prvek $e \in A$ se nazývá neutrální prvek této operace, právě když

$\forall a \in A; a * e = e * a = a$. [1]

Příklad 3

Předpokládejme binární operaci:

$a * b = a + (½)ab + b; a, b \in C$

$a * e = a$	$e * a = a$
$a + (½)ae + e = a$	$e + (½)ea + a = a$
$e = 0$	$e = 0$. [4]

Existence neutrálního prvku však není vlastností zcela samozřejmou pro každou binární algebraickou operaci. Například pro operaci sčítání v množinách celých, racionální a komplexních čísel je neutrálním prvkem číslo 0. Ale na množině přirozených čísel již neutrální prvek neexistuje, neboť 0 není přirozené číslo. [1]

Věta 1

V každé binární operaci existuje nejvýše jeden neutrální prvek.

Důkaz:

Budeme předpokládat neutrální prvky e a e´ binární operace *, která je definovaná v množině $A \neq \emptyset$. Potom podle vztahu a * e = e * a = a platí

e * e´ = e´ * e = e

a zároveň

e´ * e = e * e´ = e´.

Z těchto dvou vztahů již plyne, že e = e´, což jsme chtěli dokázat. [1]

Definice 5 Inverzní prvek

Budiž * libovolná binární algebraická operace definovaná na množině $A \neq \emptyset$, $e \in A$ její neutrální prvek. Pak říkáme, že prvek $a^{-1} \in A$ je inverzní vzhledem k prvku $a \in A$ v operaci * právě tehdy, platí-li

$a^{-1} * a = a^{-1} * a = e$. [1]

Příklad 4

Pro ukázku inverzního prvku uvedeme příklad operace násobení na množině reálných čísel s předpokládaným neutrálním prvkem e = 1.

$a * b = ab; a, b \in R$

$a^{-1} * a = e$ $\qquad$ $a^{-1} * a = e$

$a^{-1}a = 1$ $\qquad$ $aa^{-1} = 1$

$a^{-1} = 1/a$ $\qquad$ $a^{-1} = 1/a$.

Neutrální prvek zde představuje číslo 1 a ke každému reálnému číslu $a \neq 0$ existuje vždy reálné číslo 1/a takové, že platí:

a * (1/a) = (1/a) * a = 1.

Zjistili jsme, že ke každému reálnému číslu $a \neq 0$ existuje inverzní prvek, kterým je převrácená hodnota 1/a. [4]

2 Grupy

Grupy jsou v současné matematice jedním z nejdůležitějších pojmů. Matematická disciplína, která se zabývá studiem grup, se nazývá teorie grup. Teorie grup vznikla počátkem 19. století. Za zakladatele teorie grup je považován francouzský matematik Évariste Galois, který v prvním náčrtu zformuloval to, co se dnes nazývá Galoisovou teorií. Jako příklady grup můžeme uvést operace sčítání na množině celých, resp. racionálních či reálných čísel, resp. operace násobení na uvedených množinách bez nuly, ale též grupy shodností reprodukující dané geometrické útvary nebo množiny regulárních matic vzhledem k operaci násobení. [8]

Nejprve uvedeme definice základních pojmů, jako např. grupa, pologrupa, podgrupa generovaná množinou, cyklická grupa, normální podgrupa grupy, faktor-grupa, homomorfismus, izomorfismus aj.

Poté se v této práci zaměříme na popis konečných grup malých řádů, tj. řád $n \leq 15$.

2.1 Grupoidy, pologrupy, grupy

V první části této kapitoly budeme nejprve definovat pojmy – grupa, monoid, pologrupa, grupoid.

Definice 6 Grupoid

Grupoidem budeme nazývat každou dvojici (G; *), kde G je libovolná neprázdná množina a * je libovolná v ní definovaná binární operace.

Množina G se nazývá pole grupoidu (G; *). [1]

Příklad 5

Grupoidem jsou kupříkladu:

- (N; +)…množina všech přirozených čísel s operací sčítání,
- (N; *)…množina všech přirozených čísel s operací násobení,
- (C; +)…množina všech celých čísel s operací sčítání,
- (C; *)…množina všech celých čísel s operací násobení,
- (P(A); $\cup$) a (P(A); $\cap$), kde A je libovolná množina a $\cap$, $\cup$ jsou operace sjednocení a průnik. [4]

Definice 7 Pologrupa

Grupoid se nazývá pologrupa právě tehdy, je-li * asociativní binární operace. [1]

Příklad 6

Mezi pologrupy zařadíme grupoidy:

- (N; +)…množina všech přirozených čísel s operací sčítání,
- (N; *)…množina všech přirozených čísel s operací násobení,
- (C; +)…množina všech celých čísel s operací sčítání,
- (C; *)…množina všech celých čísel s operací násobení,
- (P(A); $\cup$) a (P(A); $\cap$), kde A je libovolná množina a $\cap$, $\cup$ jsou operace sjednocení a průnik.

(C; -)…množina všech celých čísel s operací odčítání je grupoid, který již netvoří pologrupu. [4]

Definice 8 Monoid

Pologrupa (G; *) se nazývá monoid právě tehdy, má-li binární operace * v množině G neutrální prvek. [1]

Příklad 7

Jako příklad monoidu uvedeme pologrupu (P(A); $\cup$), kde neutrálním prvkem je prázdná množina.

Naopak pologrupa (N; +) již není monoidem, protože vzhledem k operaci sčítání neobsahuje neutrální prvek. [4]

Definice 9 Grupa

Monoid (G; *) se nazývá grupa právě tehdy, existuje-li ke každému prvku a z množiny G inverzní prvek a^{-1} z množiny G k prvku a v dané operaci.

Množina G se pak nazývá pole grupy. [1]

Příklad 8

Opět pro ukázku uvedeme příklad grupy, a tím může být např. monoid

- (C; +)… množina všech celých čísel s operací sčítání, kde neutrálním prvkem je číslo nula a prvkem inverzním a^{-1} k prvku a bude číslo –a. [4]

V definicích 6 - 9 jsme nepředpokládali komutativnost binární operace *, avšak ani jsme ji nevyloučili. Pokud je binární operace * navíc operací komutativní, přichází na řadu následující definice. [1]

Definice 10 Abelův grupoid (pologrupa, monoid, grupa)

Grupoid (pologrupa, monoid, grupa) (G; *) se nazývá komutativní nebo také Abelův grupoid (pologrupa, monoid, grupa) právě tehdy, je-li operace * komutativní. [1]

Definice 11 Podgrupa

Nechť (G; *) je grupa. Řekneme, že (S; *) je podgrupa grupy (G; *), jestliže

1. $\emptyset \neq S \subseteq G$
2. (S; *) je grupou.

Lemma 1

Nechť (G; *) je grupa a platí $\emptyset \neq H \subseteq G$. Potom je (H; *) podgrupou grupy (G; *) právě tehdy, když

1. $(\forall\, h \in H)\ h^{-1} \in H$
2. $(\forall\, h_1, h_2 \in H)\ h_1 * h_2 \in H$.

Věta 2

Nechť (G; *) je grupa a platí $\emptyset \neq H \subseteq G$. Potom je (H; *) podgrupou grupy (G; *) právě tehdy, když pro všechna $a, b \in H$ platí:

$a * b^{-1} \in H$.

Důkaz lemmatu 1 a věty 2 nalezne čtenář v [2] na straně 14.

Niels Henrik Abel

obrázek 1: Niels Henrik Abel

Niels Henrik Abel, norský matematik, se narodil 5. srpna 1802 a zemřel velmi mladý 16. dubna 1829. V roce 1815 začal Abel studovat katedrální školu v dnešním Oslu. Zpočátku se jevil jako obyčejný žák s neobyčejným nadáním pro matematiku a fyziku. S pomocí svého učitele Holmboa začal studovat vysokoškolské texty Eulera a Newtona. V roce 1821 vstoupil na univerzitu v Oslu, kde začal pracovat na řešení rovnic s odmocninami. Na univerzitě našel Abel svého zastánce profesora astronomie Christophera Hansteena, jehož žena se o Abela starala jako o vlastního syna. O dva roky později zveřejnil Abel dokumenty o funkcionálních rovnicích a integrálech ve vědeckém žurnálu, který založil právě Hansteen. V roce 1824 dokázal nemožnost obecného řešení rovnic pátého stupně pomocí vzorců s odmocninami.

Dne 6. dubna 1929 byly v Norsku vydány poštovní známky s portrétem Abela k výročí jeho smrti a v letech 1978 – 1985 se jeho portrét objevil i na norské 500korunové bankovce.

obrázek 2: Portrét N. H. Abela na bankovce a poštovní známce

Po Abelovi je nazývána řada matematických pojmů, jako např. Abelova grupa, Abelova sumace, Abelovo kritérium. V roce 2002 po něm byla pojmenována Abelova cena. [5]

Předvedeme několik příkladů na grupy.

Příklad 9

Na množině celých čísel vyšetříme binární operaci * definovanou předpisem

$a * b = a - 2ab + b;\ a, b \in C.$

- Komutativnost

$a * b = a - 2ab + b = b - 2ba + a = b * a,$

operace je komutativní.

- Asociativnost

$(a * b) * c = (a - 2ab + b)*c = a - 2ab + b - 2(a - 2ab + b)c + c = a + b + c - 2ab - 2bc - 2ac + 4abc,$

$a * (b * c) = a*(b - 2bc + c) = a - 2a(b - 2bc + c) + (b - 2bc + c) = a + b + c - 2ab - 2bc - 2ac + 4abc,$

operace je asociativní.

- Existence neutrálního prvku

$a * e = e * a = a$

$a - 2ae + e = a$ $\qquad$ $e - 2ea + a = a$

$e = 0$ $\qquad$ $e = 0$

existuje neutrální prvek, $e = 0$.

- Existence inverzního prvku

$a^{-1} * a = a^{-1} * a = e$

$a - 2aa^{-1} + a^{-1} = 0$ $\qquad$ $a^{-1} - 2\, a^{-1}a + a = 0$

$a^{-1} = a/(2a-1)$ $\qquad$ $a^{-1} = a/(2a-1)$

inverzní prvek existuje pouze pro $a = \{0, 1\}$. Pro jiné a inverzní prvek na dané množině neexistuje.

Závěr: binární operace * definovaná předpisem $a * b = a - 2ab + b;\ a, b \in C$, tedy operace $(C; *)$, tvoří komutativní (Abelovu) grupu jen pro $a = \{0, 1\}$. [4]

Příklad 10

Na množině celých čísel vyšetříme binární operaci * definovanou předpisem

$a * b = 2a + b;\ \ a, b \in C.$

- Komutativnost

$a * b = 2a + b \neq 2b + a = b * a,$

operace není komutativní.

- Asociativnost

$(a * b) * c = (2a + b) * c = 2\,(2a + b) + c = 4a + 2b + c,$

$a * (b * c) = a * (2b + c) = 2a + 2b + c,$

operace není asociativní.

- Existence neutrálního prvku

$a * e = e * a = a$

$2a + e = a \qquad 2e + a = a$

$e = -a \qquad e = 0$

existuje pouze levý neutrální prvek, $e = 0$.

- Existence inverzního prvku

$a^{-1} * a = e$

$2a^{-1} + a = 0$

$a^{-1} = a/2$

existuje pouze levý inverzní prvek, $a^{-1} = a/2$, a to jen v případě, že $a \in C$ je sudé číslo. Je-li $a \in C$ liché, potom k němu neexistuje ani levý inverzní prvek.

Závěr: binární operace * definovaná předpisem $a * b = 2a + b;\ \ a,b \in C$, tedy operace $(C; *)$, tvoří grupoid. [4]

2.2 Konečné grupy malých řádů

Konečnými grupami nazýváme takové grupy, které mají konečně mnoho prvků. Řád každého prvku konečné grupy je konečný a grupa je do jisté míry určena svým řádem a strukturou svých podgrup. Až do kapitoly 2.1 jsme zopakovali důležité pojmy pro tuto práci a v následující části se již zaměříme na zadané téma.

V naší práci budeme využívat množinu přirozených čísel N, popřípadě množinu nezáporných celých čísel N_0. Dalšími důležitými symboly pro tuto práci budeme užívat největší společný dělitel s označením (m, n) a dále nejmenší společný násobek s označením [m, n] dvou přirozených čísel m a n.

Pro řád konečné grupy užijeme symbol o (G) a řádem prvku g v grupě G budeme rozumět řád cyklické podgrupy {g} generované prvkem g a budeme zapisovat o (g). [3]

Definice 12 Řád grupy

Grupa (G; *) se nazývá nekonečná, je-li její nosič, tj. množina G, nekonečná; v opačném případě říkáme, že (G; *) je konečná grupa a řádem této grupy rozumíme počet prvků množiny G. [2]

Příklad 11

Velmi známou grupu tvoří množina všech zbytkových tříd Z_n podle modulu $n \in N$, $n > 1$. Tyto třídy značíme $\bar{0}, \bar{1}, \ldots \overline{n-1}$ a grupovou operaci $\oplus$ definujeme takto: Pro libovolné třídy $\bar{k}, \bar{l}$ je $\bar{k} \oplus \bar{l}$ ta zbytková třída, v níž leží celé číslo k + l. Je zřejmé, že grupa $(Z_n; \oplus)$ má právě n prvků pro každé $n > 1$ a že jejím generátorem je třída $\bar{1}$. Nalezli jsme tedy pro každé $n \in N$ jeden exemplář grupy, a to grupu cyklickou.

Definice 13 Index podgrupy

Indexem podgrupy H v grupě G budeme rozumět počet tříd v levém, resp. pravém, rozkladu grupy G podle podgrupy H. Značíme [G: H]. [2]

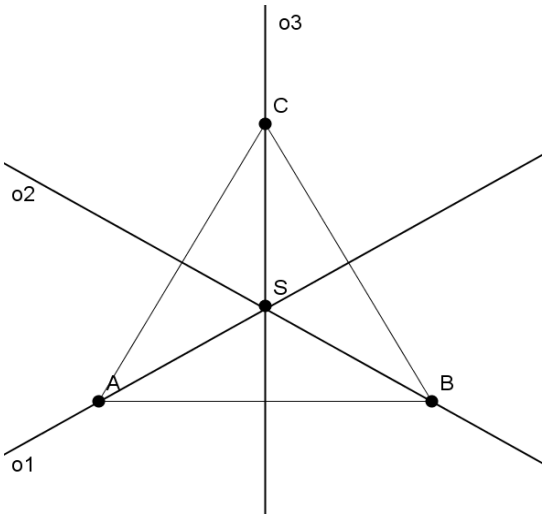
Definice 14 Normální podgrupa

Řekneme, že podgrupa H grupy G je normální podgrupou grupy G (značíme $H \Delta G$), jestliže pro každé $g \in G$ je gH = Hg. Jednotková grupa a grupa G jsou normálními podgrupami grupy G (tzv. nevlastní normální podgrupy). Všechny ostatní normální podgrupy G se nazývají vlastní. [2]

Příklad 12

Jako příklad nekomutativní grupy můžeme uvést grupu shodností v rovině reprodukujících rovnostranný trojúhelník ABC s binární operací $*$ skládání shodných zobrazení. Shodnými zobrazeními v rovině, která zobrazují trojúhelník ABC na sebe, jsou identita (Id), tři osové souměrnosti (o_1, o_2, o_3) podle os o_1, o_2, o_3 (viz obr. 1) a rotace (R, R^2) se středem S o 120 °, resp. 240 °, přičemž pro tento příklad budeme předpokládat rotaci v protisměru hodinových ručiček.

Uveďme pro toto zobrazení obrázek a operační tabulku.



obrázek 3: Shodná zobrazení trojúhelníku ABC

$*$	Id	o_1	o_2	o_3	R	R^2
Id	Id	o_1	o_2	o_3	R	R^2
o_1	o_1	Id	R^2	R	o_3	o_2
o_2	o_2	R	Id	R^2	o_1	o_3
o_3	o_3	R^2	R	Id	o_2	o_1
R	R	o_2	o_3	o_1	R^2	Id
R^2	R^2	o_3	o_1	o_2	Id	R

tabulka 1: Operační tabulka shodných zobrazení

Utvoříme všechny levé třídy gH grupy G podle podgrupy H a prověříme, zda gH = Hg u jednotlivých tříd:

$Id\ H = \{Id, R, R^2\} = H\ Id$

$R\ H = \{R, R^2, Id\} = H\ R$

$R^2\ H = \{R^2, Id, R\} = H\ R^2$

$o_1\ H = \{o_1, o_2, o_3\} = H\ o_1$

$o_2\ H = \{o_2, o_3, o_1\} = H\ o_2$

$o_3\ H = \{o_3, o_1, o_2\} = H\ o_3$.

Dokázali jsme, že gH = Hg a nyní můžeme vyslovit, že H je normální podgrupou grupy G, tj. $H \Delta G$. [2]

Symbol [G: H] bude označovat, dle definice, index podgrupy H v grupě G. Bude-li navíc H normální podgrupou grupy G, budeme dle definice zapisovat $H \Delta G$. [3]

Věta 3

Tato věta nám říká, že podmínky, které uvedeme, jsou ekvivalentní s definicí normální podgrupy.

1. $H \Delta G$
2. $(\forall g \in G)\ (\forall h \in H)\ g^{-1}hg \in H$
3. $(\forall g \in G)\ (\forall h \in H)\ g\ hg^{-1} \in H$
4. $(\forall g \in G)\ gHg^{-1} \subseteq H$
5. $(\forall g \in G)\ g^{-1}Hg \subseteq H$

Věta 4

Budiž (G; *) grupa G s binární operací * a H_i, $i \in I$, systém normálních podgrup grupy G, přičemž $I \neq \emptyset$. Potom průnik tohoto systému normálních podgrup grupy G je opět normální podgrupou grupy G.

Věta 5

Budiž H je podgrupou grupy G s binární operací *, (G; *). Je-li H normální podgrupou grupy G, potom rovnost $g_1H \circ g_2H = (g_1 * g_2)\ H$ definuje binární operaci ° na množině levých tříd grupy G podle podgrupy H.

Věta 6

Budiž H je normální podgrupou grupy G s binární operací *, (G; *). Potom množina všech levých tříd grupy G podle podgrupy H tvoří vzhledem k operaci násobení tříd $g_1H \circ g_2H = (g_1 * g_2)H$ grupu.

Důkazy vět 3 – 6 nebudeme provádět, čtenář je nalezne v literatuře [2] na straně 36, 37.

Definice 15 Faktor-grupa

> Buď H normální podgrupa grupy G. Množina všech levých tříd grupy G podle podgrupy H spolu s binární operací ° definovanou předpisem
>
> $g_1H \circ g_2H = (g_1 * g_2)H$
>
> se nazývá faktorovou grupou (faktor-grupou) grupy G podle normální podgrupy H. Značíme G/H. [2]

Věta 7 *(Lagrangeova věta)*

Budiž H podgrupa konečné grupy G. Potom $o(G) = o(H) \cdot [G: H]$, přičemž o (G) a o (H) označují řády grup G a H. [2]

Důsledkem Lagrangeovy věty je následující tvrzení:

Buď G konečná grupa, $g \in G$. Potom o (g) dělí o (G), tj. řád prvku g dělí řád grupy G.

Naším úkolem v této práci bude popsat všechny konečné grupy až do řádu $n \leq 15$. Co pro nás bude důležité je, že pro každé přirozené číslo n existuje aspoň jedna grupa řádu n. Touto grupou budeme rozumět cyklickou grupu řádu n. [3]

Definice 16 Cyklická grupa

> Buď M podmnožina grupy G. Průnik všech podgrup grupy G obsahující množinu M nazýváme podgrupou generovanou množinou M a značíme {M}. Jestliže {M} = G, pak M nazýváme množinou generátorů grupy G. Grupa G generovaná jednoprvkovou množinou {g} se nazývá cyklická. [2]

Věta 8

Každá grupa prvočíselného řádu je cyklická.

Důkaz:

Nechť G je grupa prvočíselného řádu p a $g \neq 1$ libovolný její prvek. Podle důsledku Lagrangeovy věty dělí řád prvku g prvočíslo p, a je tedy roven p. Pak ovšem G = {g}.

Věta 9

Grupa G nemá žádné vlastní podgrupy právě když je grupou prvočíselného řádu.

Důkaz:

Nechť G je grupou prvočíselného řádu a $1 \neq H \subseteq G$ buď podgrupa grupy G. Buď $1 \neq h \in H$ libovolný prvek. Podle důkazu věty 8 platí $G = \{h\} \subseteq H$, takže G = H. Grupa G nemá tedy vlastní podgrupy.

Jestliže tedy grupa G nemá žádné vlastní podgrupy, je cyklická a $1 \neq g \in G$ je libovolný prvek takový, že $\{g\} = G$. S přihlédnutím na to, že nekonečná cyklická grupa má dokonce nekonečně mnoho vlastních podgrup, musí být grupa G konečnou cyklickou grupou. Jestliže grupa G nemá vlastní normální podgrupy, nazývá se jednoduchá grupa.

Ve studiu teorie grup jsou jednoduché grupy velmi důležité. Jsou v jistém smyslu stavebními prvky, z nichž jsou „vystavěny“ větší grupy. Existují totiž grupové konstrukce, které umožňují z menších grup „vystavět“ grupu větší. Ovšem nalezení všech jednoduchých grup v oblasti nekomutativních grup by bylo extrémně obtížné. [3]

3 Homomorfizmus a izomorfizmus

Pojmy homomorfizmus a izomorfizmus představují v algebře zvláštní druh zobrazení jedné algebraické struktury do jiné. Jsou specifické tím, že si zachovávají určité vlastnosti. Například v geometrii bychom si homomorfizmus mohli představit jako dva podobné trojúhelníky a stejně tak izomorfizmus jako dva shodné trojúhelníky. Z geometrie víme, že podobnost trojúhelníků zachovává jen některé vlastnosti, oproti tomu shodnost zachovává vlastnosti všechny. Stejné to bude i s algebraickými strukturami. [4]

Definice 17 Izomorfizmus

Řekneme, že dvě grupy (G; *) a (H; °) jsou izomorfní, jestliže existuje vzájemně jednoznačné zobrazení $\varphi: G \to H$ takové, že pro všechna a, b $\in$ G platí

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

Značíme G $\cong$ H. Zobrazení φ se nazývá izomorfizmus. [2]

Věta 10

Každá nekonečná cyklická grupa je izomorfní a aditivní grupou (Z; +).

Důkaz:

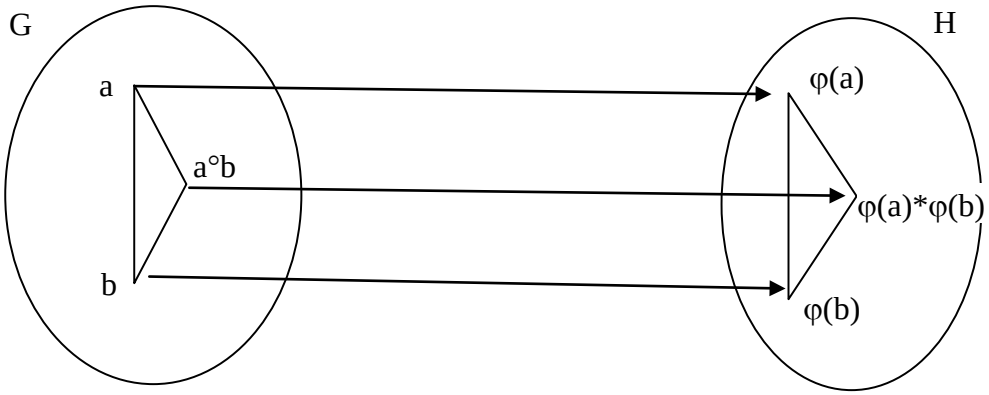
Předpokládejme, že G je nekonečná cyklická grupa s generátorem g. Potom G obsahuje všechny mocniny g^z, z $\in$ Z, a tyto mocniny jsou navzájem různé. Nadefinujeme zobrazení $\varphi: Z \to G$ předpisem $\varphi (z) = g^z$. Ovšem zobrazení φ je surjektivní, prosté a navíc $\varphi (z_1 + z_2) = g^{z1 + z2} = g^{z1} \cdot g^{z2} = \varphi (z_1) \cdot \varphi (z_2)$, což udává, že se jedná o izomorfizmus.

Definice 18 Homomorfizmus

Buďte (G; °) a (H; *) dvě grupy. Řekneme, že zobrazení φ je homomorfizmem grupy (G; °) do (H; *), jestliže

a) φ je zobrazení množiny G do H

b) $(\forall a, b \in G) \varphi (a \circ b) = \varphi (a) * \varphi (b)$. [2]



obrázek 4: Homomorfizmus

Věta 11

Nechť (G; °) a (H; *) jsou grupy a zobrazení $\varphi: G \to H$ je homomorfizmus. Potom

1. $\varphi(e) = e'$ (a sice neutrální prvek grupy G se zobrazuje na neutrální prvek v grupě H),
2. $(\forall g \in G)\ \varphi(g^{-1}) = (\varphi(g))^{-1}$.

Důkaz:

1. Pro důkaz budeme předpokládat, že e je jednotkový prvek grupy G, kde $e \circ e = e$. Potom $\varphi(e) * \varphi(e) = \varphi(e)$.

   V grupě H pro neutrální prvek e´ platí $\varphi(e) * e' = e' * \varphi(e) = \varphi(e)$. Použijeme zákon o krácení a vyjde nám $e' = \varphi(e)$.

2. Pro druhou část důkazu bude předpokladem $e' = \varphi(g \circ g^{-1}) = \varphi(g) * \varphi(g^{-1})$ a taktéž $e' = \varphi(g^{-1} \circ g) = \varphi(g^{-1}) * \varphi(g)$. Snadno nahlédneme, že v grupě (H; *) je inverzním prvkem k $\varphi(g)$ prvek $(\varphi(g))^{-1} = \varphi(g^{-1})$. [2]

Příklad 13

Nechť (G; °) a (H; *) jsou grupy a 1 resp. 1´ jejich neutrální prvky. Definujeme zobrazení $\varphi: G \to H$ tak, že pro každé $g \in G$ položíme $\varphi(g) = 1'$. Potom φ je homomorfizmus.

Jsou-li $a, b \in G$, potom $\varphi(a \circ b) = 1'$, $\varphi(a) * \varphi(b) = 1' * 1' = 1'$.

Příklad 14

Nechť $\varphi: Z \to Z$, $\varphi(a) = 3 \cdot a$, pro každé $a \in Z$. Potom φ je homomorfizmus.

Jsou-li $a, b \in Z$, potom $\varphi(a + b) = 3 \cdot (a + b) = 3a + 3b = \varphi(a) + \varphi(b)$. [7]

Definice 19 Obraz množiny, obraz homomorfizmu

Buď φ homomorfizmus grupy $(G; \circ)$ do grupy $(G'; *)$. Je-li množina H podmnožinou množiny G, $H \subseteq G$, pak $\varphi(H) = \{\varphi(h); h \in H\}$ nazýváme obrazem množiny H při homomorfizmu φ. Obraz celé grupy G nazýváme obrazem homomorfizmu φ a značíme Im φ. [2]

Věta 12

Nechť zobrazení φ je homomorfizmus grupy $(G; \circ)$ do grupy $(G'; *)$. Potom:

1. je-li H podgrupa grupy G, je $\varphi(H)$ podgrupa grupy G´
2. Im φ je podgrupa grupy G´
3. je-li $H \Delta G$, potom $\varphi(H) \Delta$ Im φ.

Důkaz:

1. Předpokládejme dva prvky $a', b' \in \varphi(H)$ a chceme předvést, že $a' \cdot b'^{-1} \in \varphi(H)$. Nechť $a, b \in H$ jsou určité prvky a platí $\varphi(a) = a'$, $\varphi(b) = b'$. Potom $\varphi(a \circ b^{-1}) = \varphi(a) * \varphi(b^{-1}) = \varphi(a) * (\varphi(b))^{-1} = a' \cdot b^{-1} \in \varphi(H)$, což znamená, že $\varphi(H)$ je podgrupou grupy G´.

2. Pokud bychom za H zvolili grupu G, znamená to, že druhá část důkazu vyplývá z části 1.

3. V poslední části chceme dokázat, že $\varphi(H) \Delta$ Im φ, použijeme k tomu větu 3. Nechť $g' \in$ Im φ a $h' \in \varphi(H)$ jsou libovolné prvky, pro které platí $g' = \varphi(g)$ pro určitý prvek $g \in G$ a $h' = \varphi(h)$ pro určitý prvek $h \in H$. Vzhledem k tomu, že H je normální podgrupou G, $H \Delta G$, platí $g^{-1} \circ h \circ g \in H$, tudíž $\varphi(g^{-1} \circ h \circ g) = \varphi(g^{-1}) * \varphi(h) * \varphi(g) = (\varphi(g))^{-1} * h' * g' \in \varphi(H)$. [2]

Definice 20 Úplný vzor množiny H´, jádro homomorfizmu

Buď φ homomorfizmus grupy (G; °) do grupy (G´; *), H´ podmnožinou G´. Množinu φ^{-1} (H´) = {g ∈ G; φ (g) ∈ H´} nazýváme úplným vzorem množiny H´ při homomorfizmu φ. Množinu φ^{-1} (e´) = {g ∈ G; φ (g) = e´} nazýváme jádrem homomorfizmu φ a značíme Ker φ (přičemž e´ je neutrální prvek grupy (G´; *)). [2]

Věta 13

Nechť zobrazení φ je homomorfizmus grupy (G; °) do grupy (G´; *). Potom

1. je-li H´ podgrupa grupy G´, je φ^{-1} (H´) podgrupa grupy G
2. je-li H´ Δ G´, je φ^{-1} (H´) Δ G
3. Ker φ je normální podgrupa grupy G.

Důkaz:

1. V první části důkazu chceme dokázat, že $a \cdot b^{-1} \in \varphi^{-1}$ (H´), což podle věty 2 znamená, že φ^{-1} (H´) je podgrupa. Nechť tedy máme dva prvky a, b ∈ φ^{-1} (H´) takové, že φ (a) ∈ H´ a také φ (b) ∈ H´. Ovšem φ (a ° b^{-1}) = φ (a) * φ (b^{-1}) = φ (a) * (φ (b))$^{-1}$ ∈ H´, což znamená, že a ° $b^{-1} \in \varphi^{-1}$ (H´).

2. Podle 1. části důkazu je φ^{-1} (H´) je podgrupou a nyní máme dokázat, že φ^{-1} (H´) je normální podgrupou. V této části budeme dokazovat, že g^{-1} ° h ° g ∈ φ^{-1} (H´) a využijeme k tomu větu 3. Nechť máme libovolné prvky g ∈ G a h ∈ φ^{-1} (H´), potom φ (g^{-1} ° h ° g) = = φ (g^{-1}) * φ (h) * φ (g) ∈ H´. Jelikož φ (h) ∈ H´ a H´ Δ G, potom g^{-1} ° h ° g ∈ φ^{-1} (H´).

3. Pokud bychom zvolili H´ = ({e´}; *), 3. část důkazu by plynula z části 2. [2]

Na počátku této kapitoly jsme homomorfizmus v geometrii přirovnali ke dvěma podobným trojúhelníkům. Nyní si v následující větě uvedeme některé vlastnosti, které se homomorfním zobrazením zachovávají.

Věta 14

Nechť grupa (G; °) je homomorfním obrazem grupy (H; *), potom platí:

1. je-li operace * komutativní, je i operace ° komutativní
2. je-li operace * asociativní, je i operace ° asociativní
3. má-li operace * neutrální prvek, má i operace ° neutrální prvek.

Důkaz:

V důkazu jednotlivých vlastností budeme předpokládat, že $x, y, z \in H$ a nechť $\varphi(x) = a$, $\varphi(y) = b$, $\varphi(z) = c \in G$.

1. Komutativnost algebraických struktur:

$a \circ b = \varphi(x) \circ \varphi(y) = \varphi(x * y) = \varphi(y * x) = \varphi(y) \circ \varphi(x) = b \circ a.$

2. Asociativnost algebraických struktur:

$a \circ (b \circ c) = \varphi(x) \circ [\varphi(y) \circ \varphi(z)] = \varphi(x) \circ [\varphi(y * z)] = \varphi[x * (y * z)] = \varphi[(x * y) * z] =$
$= [\varphi(x * y)] \circ \varphi(z) = [\varphi(x) \circ \varphi(y)] \circ \varphi(z) = (a \circ b) \circ c.$

3. Nechť e je neutrálním prvkem algebraické struktury $(H; *)$ a $\varphi(e)$ je neutrálním prvkem algebraické struktury $(G; \circ)$, potom pro pravou neutrálnost platí

$a \circ \varphi(e) = \varphi(x) \circ \varphi(e) = \varphi(x * e) = \varphi(x) = a,$

levá neutrálnost je analogická, a sice:

$\varphi(e) \circ a = \varphi(e) \circ \varphi(x) = \varphi(e * x) = \varphi(x) = a.$ [4]

4 Konečné grupy

Jak jsme již zmínili na začátku této kapitoly budeme klást důraz na konečné grupy řádu $n \leq 15$. V kapitole 2. 2 jsme již dokázali popsat grupy řádu 2, 3, 5, 7, 11, 13. Nyní se budeme věnovat studiu grup řádu 4. [3]

4.1 Grupy řádu 4

Následující lemma nám usnadní práci při studování grup řádu 4 a později i řádu 8.

Lemma 2

Nechť G je taková grupa, v níž pro každý prvek a platí $a^2 = 1$. Potom G je Abelova grupa.

Důkaz:

Nechť existují dva libovolné prvky a, b, které náleží grupě G. Vynásobíme-li vztah $1 = (ab)^2 = abab$ prvkem ba zleva, dostaneme $ba = baabab$. Jestliže platí $a^2 = b^2 = 1$, potom je rovnost ba = ab dokázána. [3]

Studium grup řádu 4 můžeme rozdělit na dvě části.

(1) V první části uvedeme grupu G, ve které existuje prvek řádu 4. To pro nás znamená, že jde o cyklickou čtyřprvkovou grupu a snadno napíšeme operační tabulku.

	1	a	a^2	a^3
1	1	a	a^2	a^3
a	a	a^2	a^3	1
a^2	a^2	a^3	1	a
a^3	a^3	1	a	a^2

tabulka 2: Cyklická grupa řádu 4

(2) Pokud ale grupa G neobsahuje prvek řádu 4, potom z důsledku Lagrangeovy věty plyne, že všechny nejednotkové prvky mají řád 2 a podle lemmatu 1 je grupa G komutativní.

Označíme-li dva nejednotkové prvky a, b z grupy G takové, že $a \neq b$, pak v grupě G musí platit rovnost $a^2 = b^2 = 1$ a $ab = ba$. Vzhledem k těmto vztahům můžeme napsat operační tabulku. Touto tabulkou je zadána tzv. Kleinova čtyřgrupa. [3]

	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

tabulka 3: Necyklická grupa řádu 4

4.2 Grupy řádu 6

V následujícím odstavci prostudujeme grupy řádu 6, které stejně jako předcházející rozdělíme na dvě části.

(1) V první části opět uvedeme grupu G, ve které existuje prvek řádu 6. Snadno nahlédneme, že jde opět o cyklickou grupu řádu 6, pro kterou uvedeme operační tabulku.

	1	a	a^2	a^3	a^4	a^5
1	1	a	a^2	a^3	a^4	a^5
a	a	a^2	a^3	a^4	a^5	1
a^2	a^2	a^3	a^4	a^5	1	a
a^3	a^3	a^4	a^5	1	a	a^2
a^4	a^4	a^5	1	a	a^2	a^3
a^5	a^5	1	a	a^2	a^3	a^4

tabulka 4: Cyklická grupa řádu 6

(2) Ve druhé části se budeme opět věnovat necyklické grupě řádu 6, z čehož plyne, že její nejednotkové prvky budou mít řád 2 nebo řád 3.

Avšak řád 2 musíme vyloučit, neboť by v grupě G existovaly pouze nejednotkové prvky řádu 2, např. $a \neq b$. Potom by to znamenalo, že grupa G obsahuje Kleinovu čtyřgrupu, což ale dle Lagrangeovy věty není možné.

V grupě G musí tedy existovat prvek řádu 3, a sice existuje prvek $a \neq 1$ takový, že $a^3 = 1$. Grupa G musí mimo prvků 1, a, $a^2 = b$ obsahovat navíc ještě prvek c takový, že $ac = d$ a $a^2c = e$. Tímto jsme dostali šest prvků, které potřebujeme, pro konstrukci cyklické grupy řádu 6.

Následně předvedeme, že $c^2 = 1$, $d^2 = 1$ a také $e^2 = 1$. Jelikož je prvek c různý od prvků 1, a i a^2, a v grupě G platí zákon krácení jak zprava tak zleva, vyloučíme možnosti $c^2 = c$, $c^2 = ac$ i $c^2 = a^2c$, poněvadž by vedly ke sporu. Pokud bychom připustili, že $c^2 \neq 1$, musel by prvek c

mít řád 3, což by znamenalo $c^3 = 1$. Ovšem dostáváme se do sporu s tím, že pokud by se $c^2 = a$, platilo by $1 = c^3 = ac = d$, což je spor. Stejně tak kdyby se $c^2 = a^2$, platilo by $1 = c^3 = a^2c = e$, což je opět spor. Proto tedy platí, že $c^2 = 1$.

Analogicky předvedeme, že $d^2 = 1$, resp. $e^2 = 1$. Stejně jako v předchozím odstavci, tak i prvek d, resp. e musí být různý od prvků 1, a i a^2. Avšak stále v grupě G platí zákon krácení zprava i zleva, tak opět vyloučíme takové možnosti, že $d^2 = d$, $d^2 = ad$ i $d^2 = a^2d$, resp. $e^2 = e$, $e^2 = ae$ i $e^2 = a^2e$. Kdyby neplatilo, že $d^2 = 1$, resp. $e^2 = 1$, potom by prvek d, resp. e musel mít řád 3, přičemž by platilo $d^3 = 1$, resp. $e^3 = 1$.

Získáváme opět spor, a to takový, že pokud by se $d^2 = a$, resp. $e^2 = a$, platilo by $1 = d^3 = ad = e$, resp. $1 = e^3 = ae = c$. I možnost, že se $d^2 = a^2$, resp. $e^2 = a^2$ vede ke sporu, muselo by platit $1 = d^3 = a^2d = c$, resp. $1 = e^3 = a^2e = d$. Což pro nás znamená, že $d^2 = e^2 = 1$.

	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	b	1	d	e	c
b	b	1	a	e	c	d
c	c	e	d	1	b	a
d	d	c	e	a	1	b
e	e	d	c	b	a	1

tabulka 5: Necyklická grupa řádu 6

Z této tabulky je zřejmé, že se jedná o nekomutativní algebraickou strukturu. Zda-li se jedná skutečně o grupu, to provedeme bezprostředně pomocí tabulky, ovšem s kontrolou asociativnosti to bude obtížnější. Podle [3] nám vyjde, že zobrazení $\varphi(1) = Id$, $\varphi(a) = (123)$, $\varphi(b) = (132)$, $\varphi(c) = (12)$, $\varphi(d) = (23)$ a $\varphi(e) = (13)$ je izomorfizmem G na S_3, přičemž S_3 je symetrická grupa stupně 3. [3]

Definice 21 Symetrická grupa stupně n

Symetrickou grupou stupně n rozumíme množinu všech permutací množiny M = {1, 2,., n} spolu s operací skládání permutací. [3]

Definice 22 Skládání permutací

Operaci skládání permutací definujeme pomocí vztahu takto

$\pi_1\pi_2(i) = \pi_2(r_i)$, kde $r_i = \pi_1(i)$, i = 1, 2, …, n. [3]

Těmito jednotlivými prostředky jsme zjistili, že každá grupa řádu 6 je izomorfní buď s cyklickou grupou řádu 6 (Z_6), nebo se symetrickou grupou stupně 3 (S_3).

Avšak s rostoucím řádem nám jistě narůstají i potíže při konstrukci grupy. Proto nyní uvedeme definice, ve kterých bude zachycen postup, jak pomocí grup nižšího řádu zkonstruovat grupy vyššího řádu. [3]

Definice 23 Vnější direktní součin

Nechť H, K jsou grupy. Množina G všech uspořádaných dvojic (h, k), $h \in H$, $k \in K$, spolu s binární operací $(h_1, k_1) \cdot (h_2, k_2) = (h_1h_2, k_1k_2)$ je opět grupou, kterou nazýváme vnějším direktním součinem grup H a K a zapisujeme G = H x K. [3]

Definice 24 Vnitřní direktní součin

Nechť H, K jsou dvě normální podgrupy grupy G. Jestliže $H \cup K = G$ a $H \cap K = 1$, říkáme, že grupa G je vnitřním direktním součinem grup H a K a zapisujeme G = H x K. [3]

Lemma 3

Grupa G je direktním součinem svých podgrup H, K právě když pro každé $h \in H$, $k \in K$ platí hk = kh a každý prvek $g \in G$ lze psát jednoznačně až na pořadí ve tvaru g = hk, $h \in H$, $k \in K$. [3]

V předchozích definicích jsme však uvedli dvě definice na direktní součin, a sice na vnější direktní součin a vnitřní direktní součin. Ovšem tyto dva pojmy není třeba rozlišovat a to si ukážeme právě v následujícím odstavci.

Buď H, K dvě grupy a G = H x K jejich vnější direktní součin. Jestliže označíme $H' = \{(h, 1), h \in H\}$, je zobrazení $\varphi(h) = (h, 1)$ izomorfizmem H na H′ a $H \cong H'$. Stejně budeme postupovat i pro K, označme $K' = \{(1, k), k \in K\}$, potom je zobrazení $\varphi(k) = (1, k)$ izomorfizmem K na K′a $K \cong K'$. Rovnost $(h, 1) \cdot (1, k) = (h, k) = (1, k) \cdot (h, 1)$ ukazuje, že G je vnitřním direktním součinem grup H′, K′, což znamená grup izomorfních s grupami H, K.

Kdybychom chtěli postupovat opačně, bylo by G vnitřní direktní součin svých podgrup H, K. Pokud by ale G′ bylo vnějším direktním součinem grup H, K, tak by se $G' \cong G$ (zobrazení $\varphi(h, k) = hk$, kdy $H' \cong H$ a $K' \cong K$).

Věta 15

Nechť existují dvě cyklické grupy řádů m a n, jenž jsou nesoudělné. Direktní součin těchto dvou grup je opět cyklická grupa řádu mn.

Důkaz:

Budiž H = {a} je cyklická grupa řádu m a K = {b} je cyklická grupa řádu n. Potom direktní součin G = H x K obsahuje prvky ve tvaru $a^r b^s$, kde $0 \leq r < m$, $0 \leq s < n$, a tudíž $o(G) \leq mn$.

Následně předvedeme, že prvek ab má v grupě G řád mn. Platí $(ab)^{mn} = a^{mn} \cdot b^{mn} = 1$. Pokud by pro jisté t bylo $(ab)^t = 1$, potom je $1 = (ab)^{mt} = a^{mt} \cdot b^{mt} = b^{mt}$, takže $n \mid mt$ a vzhledem k (n, m) = 1 $n \mid t$. Analogicky dokážeme říci, že $m \mid t$, a tedy $[m, n] \mid t$. Avšak čísla m, n jsou však nesoudělná, a proto nejmenší společný násobek [m, n] = mn. Z toho vyplývá, že řád prvku ab v grupě G je mn a G = {ab}. [3]

5 Konečné komutativní grupy

Ve studiu teorie grup je komutativní grupou taková grupa, ve které pro všechny prvky a, b z grupy G platí, že a * b = b * a. Komutativní grupy se nazývají Abelovy grupy.

Všechny konečné grupy, které mají prvočíselný řád, jsou automaticky komutativní, neboť jsou cyklické. [8]

Definice 25 Periodická Abelova grupa

Abelova grupa G nemající prvky nekonečného řádu se nazývá periodická. [3]

Věta 16

Budiž G libovolná Abelova grupa. Potom množina, kterou označíme

$G_p = \{g \in G, o(g) = p^k, k \in N_0\}$, kde p je prvočíslo, je podgrupou grupy G.

Důkaz:

Nechť existují prvky $g, h \in G_{p1}$ a nechť $o(g) = p^r$ a $o(h) = p^s$, přičemž $r \geq s$.

Potom i prvek $g^{-1} \in G_p$, neboť $o(g^{-1}) = p^r$. Také prvek $gh \in G_p$, neboť $(gh)^{pr} = g^{pr} \cdot h^{pr} = 1$, tudíž $o(gh) \leq p^r$.

Definice 26 P-grupa

Konečná grupa řádu p^n, kde $n \in N$, a p je prvočíslo, se nazývá p-grupou. [3]

Věta 17

Pro každou periodickou grupu platí, že je direktním součinem svých p-primárních komponent.

Věta 18

Nechť G je Abelova p-grupa a a je její prvek s maximálním řádem p^k. Potom je cyklická grupa {a} direktním činitelem v grupě G. To znamená, že G = {a} x H. (Skutečnost, že a je prvek maximálního řádu v grupě G znamená, že pro všechna $g \in G$ platí $o(g) \leq p^k$).

Věta 19

Pro každou konečnou Abelovu p-grupu platí, že je direktním součinem cyklických grup.

Důkaz:

Má-li grupa G řád p, potom podle věty 8 tvoří cyklickou grupu. Nechť má tedy grupa G řád p^n, kde $n > 1$. Budeme předpokládat, že každá Abelova p-grupa řádu menšího než p^n, je již direktním součinem cyklických grup. Je-li $a \in G$ prvek maximálního řádu v grupě G, pak je podle věty 18 G = {a} x H. Nicméně H je podle indukčního předpokladu direktním součinem cyklických grup, což dokončuje důkaz.

Věta 20

Nechť existuje konečná Abelova p-grupa G. Jestliže je grupa G direktním součinem cyklických grup, $G = Z_{pk1} \times Z_{pk2} \times \ldots \times Z_{pkn}$, potom jsou čísla $k_1, k_2, \ldots, k_n$ určena grupou G jednoznačně.

Je-li G konečná Abelova grupa, užití vět 17 a 19 zajistí existenci direktního rozkladu. Řády cyklických direktních činitelů jsou přitom určeny jednoznačně a tyto řády nazýváme invarianty grupy G. Nechť máme dvě konečné Abelovy grupy, potom jsou izomorfní, právě když mají stejné soustavy invariantů. Ke každé soustavě invariantů existuje jistá konečná komutativní grupa, jejíž soustava invariantů se rovná předem zadané soustavě invariantů.

Nyní uvedeme postup, který je potřeba pro nalezení komutativních grup řádu n.

1) Je-li $n = p_1^{k1} \cdot p_2^{k2} \cdot \ldots \cdot p_r^{kr}$, kde zápis čísla n je v kanonickém tvaru a dále je-li G podle věty 17 direktním součinem svých p_i – primárních komponent G_{pi}, pro i = 1, 2, …,r.

2) Pomocí věty 19 je každá G_{pi} direktním součinem cyklických grup s řády p_i^{ki1}, p_i^{ki2},.., p_i^{kis}; kde $k_{i1} + k_{i2} + \ldots + k_{isi} = k_i$, i = 1, 2, …r, $s_i \in N$.

Pro nalezení všech možných direktních rozkladů komponenty G_{pi} je nejprve nutné nalézt všechna vyjádření čísla k_i ve tvaru součtu několika sčítanců z N.

3) Využitím věty 15 dospějeme ke zjednodušení direktního rozkladu grupy G. [3]

5.1 Konečné komutativní grupy neprvočíselného řádu

5.1.1 Konečné grupy řádu 4

Pro n = 4 můžeme dostat následují invarianty:

I. $2^1, 2^1$ $G = Z_2 \times Z_2$

II. 2^2 $G = Z_4$

jestliže se zaměříme na variantu I., potom dostáváme dvě grupy, které již byly v naší práci sestrojené (viz tabulka 2). U části II. však dostáváme cyklickou grupu řádu 4 (viz tabulka 1).

5.1.2 Konečné grupy řádu 6

Pro n = 6 dostaneme následující invarianty:

I. $2^1, 3^1$ $G = Z_2 \times Z_3 \cong Z_6$

dle věty 15 je jasné, že existuje jediná komutativní grupa, a to cyklická grupa řádu 6 (viz tabulka 3).

5.1.3 Konečné grupy řádu 8

Pro n = 8 již dostáváme tři následující invarianty:

I. 2^3 $G = Z_8$

II. $2^2, 2^1$ $G = Z_4 \times Z_2$

III. $2^1, 2^1, 2^1$ $G = Z_2 \times Z_2 \times Z_2$

možnost I. udává cyklickou grupu řádu 8.

	1	a	a^2	a^3	a^4	a^5	a^6	a^7
1	1	a	a^2	a^3	a^4	a^5	a^6	a^7
a	a	a^2	a^3	a^4	a^5	a^6	a^7	1
a^2	a^2	a^3	a^4	a^5	a^6	a^7	1	a
a^3	a^3	a^4	a^5	a^6	a^7	1	a	a^2
a^4	a^4	a^5	a^6	a^7	1	a	a^2	a^3
a^5	a^5	a^6	a^7	1	a	a^2	a^3	a^4
a^6	a^6	a^7	1	a	a^2	a^3	a^4	a^5
a^7	a^7	1	a	a^2	a^3	a^4	a^5	a^6

tabulka 6: Cyklická grupa řádu 8

Možnost II. nám říká, že první cyklická grupa řádu 4 je generovaná např. prvkem a, kde $a^4 = 1$ a druhá je generovaná např. prvkem b, kde $b^2 = 1$. Nesmíme však zapomenout, že ab = ba.

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	ab	a^2b	a^3b	1	a	a^2	a^3
ab	ab	a^2b	a^3b	b	a	a^2	a^3	1
a^2b	a^2b	a^3b	b	ab	a^2	a^3	1	a
a^3b	a^3b	b	ab	a^2b	a^3	1	a	a^2

tabulka 7: Komutativní grupa $G = Z_4 \times Z_2$

Poslední možnost III., kde první grupa je generovaná např. prvkem a, druhá např. prvkem b a třetí např. prvkem c platí $a^2 = b^2 = c^2 = 1$ a zároveň ab = ba, ac = ca, bc = cb.

	1	a	b	c	ab	ac	bc	abc
1	1	a	b	c	ab	ac	bc	abc
a	a	1	ab	ac	b	c	abc	bc
b	b	ab	1	bc	a	abc	c	ac
c	c	ac	bc	1	abc	a	b	ab
ab	ab	b	a	abc	1	bc	ac	c
ac	ac	c	abc	a	bc	1	ab	bc
bc	bc	abc	c	b	ac	ab	1	a
abc	abc	bc	ac	ab	c	b	a	1

tabulka 8: Komutativní grupa $G = Z_2 \times Z_2 \times Z_2$

5.1.4 Konečné grupy řádu 9

Jediné možné invarianty pro n = 9 jsou:

I. 3^2 $G = Z_9$

II. $3^1, 3^1$ $G = Z_3 \times Z_3$

případem I. je opět určena cyklická grupa řádu 9.

	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
1	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
a	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	1
a^2	a^2	a^3	a^4	a^5	a^6	a^7	a^8	1	a
a^3	a^3	a^4	a^5	a^6	a^7	a^8	1	a	a^2
a^4	a^4	a^5	a^6	a^7	a^8	1	a	a^2	a^3
a^5	a^5	a^6	a^7	a^8	1	a	a^2	a^3	a^4
a^6	a^6	a^7	a^8	1	a	a^2	a^3	a^4	a^5
a^7	a^7	a^8	1	a	a^2	a^3	a^4	a^5	a^6
a^8	a^8	1	a	a^2	a^3	a^4	a^5	a^6	a^7

tabulka 9: Cyklická grupa řádu 9

Avšak případ II. určuje devíti prvkovou grupu, která je direktním součinem dvou cyklických grup, z nichž první je generována např. prvkem a, kde $a^3 = 1$ a druhá je generována např. prvkem b, kde $b^3 = 1$. Zároveň nesmíme opomenout, že ab = ba.

	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
1	1	a	a^2	b	b^2	ab	a^2b	ab^2	a^2b^2
a	a	a^2	1	ab	ab^2	a^2b	b	a^2b^2	b^2
a^2	a^2	1	a	a^2b	a^2b^2	b	ab	b^2	ab^2
b	b	ab	a^2b	b^2	1	ab^2	a^2b^2	a	a^2
b^2	b^2	ab^2	a^2b^2	1	b	a	a^2	ab	a^2b
ab	ab	a^2b	b	ab^2	a	a^2b^2	b^2	a^2	1
a^2b	a^2b	b	ab	a^2b^2	a^2	b^2	ab^2	1	a
ab^2	ab^2	a^2b^2	b^2	a	ab	a^2	1	a^2b	b
a^2b^2	a^2b^2	b^2	ab^2	a^2	a^2b	1	a	b	ab

tabulka 10: Komutativní grupa $G = Z_3 \times Z_3$

5.1.5 Konečné grupy řádu 10

Číslo n = 10 poskytuje následující dvojici invariantů 2^1, 5^1.

$G = Z_2 \times Z_5 \cong Z_{10}$

což znamená, že existuje jediná komutativní grupa řádu 10, a to je cyklická grupa.

	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9
1	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9
a	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	1
a^2	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	1	a
a^3	a^3	a^4	a^5	a^6	a^7	a^8	a^9	1	a	a^2
a^4	a^4	a^5	a^6	a^7	a^8	a^9	1	a	a^2	a^3
a^5	a^5	a^6	a^7	a^8	a^9	1	a	a^2	a^3	a^4
a^6	a^6	a^7	a^8	a^9	1	a	a^2	a^3	a^4	a^5
a^7	a^7	a^8	a^9	1	a	a^2	a^3	a^4	a^5	a^6
a^8	a^8	a^9	1	a	a^2	a^3	a^4	a^5	a^6	a^7
a^9	a^9	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8

tabulka 11: Cyklická grupa řádu 10

5.1.6 Konečné grupy řádu 12

Všechny možné invarianty, kterými je tato grupa určena jsou:

I. $2^2, 3^1$ $\quad G = Z_4 \times Z_3 \cong Z_{12}$

II. $2^1, 2^1, 3^1$ $\quad G = Z_2 \times Z_2 \times Z_3$

v případě I. opět dostáváme cyklickou grupu řádu 12.

	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
1	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
a	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	1
a^2	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	1	a
a^3	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	1	a	a^2
a^4	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	1	a	a^2	a^3
a^5	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	1	a	a^2	a^3	a^4
a^6	a^6	a^7	a^8	a^9	a^{10}	a^{11}	1	a	a^2	a^3	a^4	a^5
a^7	a^7	a^8	a^9	a^{10}	a^{11}	1	a	a^2	a^3	a^4	a^5	a^6
a^8	a^8	a^9	a^{10}	a^{11}	1	a	a^2	a^3	a^4	a^5	a^6	a^7
a^9	a^9	a^{10}	a^{11}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
a^{10}	a^{10}	a^{11}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9
a^{11}	a^{11}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}

tabulka 12: Cyklická grupa řádu 12

Pro případ II. můžeme využít, že platí $Z_2 \times Z_3 \cong Z_6$, což znamená, že dostáváme $G = Z_2 \times Z_6$ a tímto dostáváme dvě cyklické grupy, z nichž první je generována např. prvkem a, kde $a^2 = 1$ a druhá je generována např. prvkem b, přičemž $b^6 = 1$. Opět ale nezapomeneme, že ab = ba.

	1	a	b	b^2	b^3	b^4	b^5	ab	ab^2	ab^3	ab^4	ab^5
1	1	a	b	b^2	b^3	b^4	b^5	ab	ab^2	ab^3	ab^4	ab^5
a	a	1	ab	ab^2	ab^3	ab^4	ab^5	b	b^2	b^3	b^4	b^5
b	b	ab	b^2	b^3	b^4	b^5	1	ab^2	ab^3	ab^4	ab^5	a
b^2	b^2	ab^2	b^3	b^4	b^5	1	b	ab^3	ab^4	ab^5	a	ab
b^3	b^3	ab^3	b^4	b^5	1	b^2	b^2	ab^4	ab^5	a	ab	ab^2
b^4	b^4	ab^4	b^5	1	b^2	b^2	b^3	ab^5	a	ab	ab^2	ab^3
b^5	b^5	ab^5	1	b	b^2	b^3	b^4	a	ab	ab^2	ab^3	ab^4
ab	ab	b	ab^2	ab^3	ab^4	ab^5	a	b^2	b^3	b^4	b^5	1
ab^2	ab^2	b^2	ab^3	ab^4	ab^5	a	ab	b^3	b^4	b^5	1	b
ab^3	ab^3	b^3	ab^4	ab^5	a	ab	ab^2	b^4	b^5	1	b	b^2
ab^4	ab^4	b^4	ab^5	a	ab	ab^2	ab^3	b^5	1	b	b^2	b^3
ab^5	ab^5	b^5	a	ab	ab^2	ab^3	ab^4	1	b	b^2	b^3	b^4

tabulka 13: Komutativní grupa $G = Z_2 \times Z_2 \times Z_3$

5.1.7 Konečné grupy řádu 14

Pro konečnou grupu řádu 14 existuje pouze jediná množina invariantů, a to 2^1, 7^1.

$G = Z_2 \times Z_7 \cong Z_{14}$

což pro nás znamená, že existuje jediná komutativní grupa řádu 14, a to grupa cyklická.

	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}
1	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}
a	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	1
a^2	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	1	a
a^3	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	1	a	a^2
a^4	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	1	a	a^2	a^3
a^5	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	1	a	a^2	a^3	a^4
a^6	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	1	a	a^2	a^3	a^4	a^5
a^7	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	1	a	a^2	a^3	a^4	a^5	a^6
a^8	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	1	a	a^2	a^3	a^4	a^5	a^6	a^7
a^9	a^9	a^{10}	a^{11}	a^{12}	a^{13}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
a^{10}	a^{10}	a^{11}	a^{12}	a^{13}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9
a^{11}	a^{11}	a^{12}	a^{13}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
a^{12}	a^{12}	a^{13}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
a^{13}	a^{13}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}

tabulka 14: Cyklická grupa řádu 14

5.1.8 Konečné grupy řádu 15

Konečná grupa řádu 15 je obdobná jako konečná grupa s řádem 14. Jediná množina invariantů je 3^1, 5^1.

$G = Z_3 \times Z_5 \cong Z_{15}$

opět existuje jediná komutativní grupa řádu 15, a to cyklická grupa. [3]

	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}
1	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}
a	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1
a^2	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1	a
a^3	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1	a	a^2
a^4	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1	a	a^2	a^3
a^5	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1	a	a^2	a^3	a^4
a^6	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1	a	a^2	a^3	a^4	a^5
a^7	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1	a	a^2	a^3	a^4	a^5	a^6
a^8	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1	a	a^2	a^3	a^4	a^5	a^6	a^7
a^9	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
a^{10}	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9
a^{11}	a^{11}	a^{12}	a^{13}	a^{14}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
a^{12}	a^{12}	a^{13}	a^{14}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}
a^{13}	a^{13}	a^{14}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}
a^{14}	a^{14}	1	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}

tabulka 15: Cyklická grupa řádu 15

6 Konečné nekomutativní grupy

Zatím jsme v naší práci pracovali s komutativními grupami. Avšak existují i nekomutativní grupy a těm se budeme věnovat v následující části. Uvedeme několik vět pro výpočet nekomutativních grup a předvedeme i některé výpočty. [3]

6.1 Nekomutativní grupy řádu 8

V předchozí kapitole jsme popsali pouze komutativní grupy řádu 8 a nyní nám zbývá popsat také nekomutativní grupy řádu 8.

Osmiprvková nekomutativní grupa nemůže obsahovat prvek řádu 8, protože by vznikla cyklická a zároveň komutativní grupa. Podle lemmatu 2 nemůže obsahovat ani nejednotkové prvky řádu 2. Je-li G taková grupa, že pro každý nejednotkový prvek a platí $a^2 = 1$, potom je grupa G Abelova. Musí tedy grupa G obsahovat prvek řádu 4, který označíme jako a. Grupa $A = \{a\}$ je cyklická grupa řádu 4, $[G : A] = 2$.

Pro tuto práci uvedeme následující tvrzení:

Nechť H je taková podgrupa grupy G, že $[G : H] = 2$. Potom $H \Delta G$.

Tedy A je normální podgrupou grupy G ($A \Delta G$) a faktor grupa G/A má řád 2. Nechť $b \in G$ je prvek takový, že $b \notin A$, potom $(bA)^2 = b^2A = A$, a tudíž $b^2 \in A$.

Již jsme ukázali, že $b^2 \in A$, což znamená, že možnosti, které můžeme dostat jsou $b^2 = 1$, $b^2 = a$, $b^2 = a^2$ a $b^2 = a^3$. Avšak $b^2 = a$ vyloučíme, protože kdyby $b^2 = a$, byla by grupa $\{b\}$ cyklickou grupou řádu 8, která obsahuje prvky 1, a, a^2, a^3, b, ab, a^2b, a^3b, což vede ke sporu. Dále možnost $b^2 = a^3$ vyloučíme také, neboť by grupa $\{b\}$ opět tvořila cyklickou grupu řádu 8 s prvky 1, a, b, ab, a^2, a^2b, a^3, a^3b.

Zbývá nám tedy prověřit možnosti $b^2 = 1$, $b^2 = a^2$. Navíc je grupa A normální podgrupa grupy G a podle věty 3 můžeme napsat $b^{-1}ab \in A$, $b^{-1}ab = a^n$, kde n = 0, 1, 2, 3. Ale variantu $b^{-1}ab = 1$ musíme vyloučit, neboť by se ab = b, což je spor a variantu $b^{-1}ab = a$ vyloučíme také, neboť po vynásobení prvkem b zleva dostáváme ab = ba, což vede ke komutativní grupě. Nyní prověříme variantu $b^{-1}ab = a^2$. Po vynásobení výrazu $b^{-1} \cdot b^{-1}ab \cdot b$ dostáváme tvar $b^{-1}a^2b = b^{-1}ab \cdot b^{-1}ab = a^2 \cdot a^2 = a^4 = 1$. Z toho plyne, že $b^{-1}a^2b = 1$, avšak po vynásobení prvkem b zleva dostaneme, že $a^2b = b$, což by ale platilo pro $a^2 = 1$, to vede ke sporu.

Poslední varianta, která nám zbývá, je $b^{-1}ab = a^3$. Po úpravě dostaneme

$b^{-1}a^3b = b^{-1}ab \cdot b^{-1}ab \cdot b^{-1}ab = a^3 \cdot a^3 \cdot a^3 = a^{3^2} = a$, odtud již $ba = a^3b$.

Snadno nahlédneme, že existují dvě nekomutativní grupy řádu 8, a sice takové, že jejich definující relace jsou následné:

(1) $a^4 = 1, b^2 = 1, b^{-1}ab = a^3$,

(2) $a^4 = 1, b^2 = a^2, b^{-1}ab = a^3$. [3]

ad (1)

Abychom mohli snadno sestrojit operační tabulku, uvedeme převod zápisů ve tvaru $ba^x = a^nb$.

Již máme $ba = a^3b$, nyní ještě $ba^2 = ba \cdot a = a^3ba = a^3a^3b = a^2b$,

$ba^3 = ba^2 \cdot a = a^2ba = a^2a^3b = ab$.

Sestrojení operační tabulky pro nekomutativní grupy řádu 8 je následovní

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

tabulka 16: Nekomutativní grupa řádu 8; $a^4 = 1, b^2 = 1, b^{-1}ab = a^3$

ad (2)

Definující relace pro druhou nekomutativní grupu řádu 8 jsme již uvedli, nyní zbývá uvést tvary prvků $ba^x = a^nb$.

$ba^3 = ab$, $ba^2 = ba^2 \cdot a^4 = ba^3 \cdot a^3 = aba^3 = aab = a^2b$,

$ba = ba \cdot a^4 = ba^2 \cdot a^3 = a^2ba^3 = a^2ab = a^3b$.

Operační tabulka pro nekomutativní grupy řádu 8 je

	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	1	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	1
a^2b	a^2b	ab	b	a^3b	1	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	1	a^3	a^2

tabulka 17: Nekomutativní grupa řádu 8; $a^4 = 1$, $b^2 = a^2$, $b^{-1}ab = a^3$

6.2 Nekomutativní grupy řádu 9

Stejně jako konečné grupy řádu 8 jsme rozdělili na komutativní a nekomutativní, tak i konečné grupy řádu 9 takto rozdělíme. To znamená, že se budeme zabývat konečnými nekomutativními grupami řádu 9. Avšak nežli začneme konstruovat tento proces, uvedeme velmi důležitou definici.

Definice 27 Centrum grupy

Buď G grupa. Množinu $Z = \{z \in G; zg = gz \text{ pro každé } g \in Z\}$ nazýváme centrum grupy G. [3]

Věta 21

Nechť G je libovolná grupa. Centrum Z grupy G je komutativní podgrupa grupy G. Navíc každá podgrupa centra grupy G je normální podgrupou grupy G.

Věta 22

Pro každou konečnou p-grupu platí, že má netriviální centrum, což znamená, že prvočíslo p dělí řád centra Z.

Nyní se vrátíme zpět ke konstrukci nekomutativních grup řádu 9. Nechť tedy máme konečnou grupu řádu 9, potom p-grupou této grupy je 3-grupa. Podgrupou této grupy je

centrum Z, přičemž vzhledem na větu 22 je tato podgrupa tříprvková či devítiprvková. Avšak druhou možnost jsme nuceni vyloučit, neboť Z = G, kde G je komutativní grupa.

Aby grupa G byla nekomutativní, musela by nutně mít tříprvkové centrum takové, že Z = {b}, přičemž $b^3 = 1$. Avšak také musí existovat prvek a takový, kde $a \in G$, $a \notin Z$. Jistě také i $a^2 \notin Z$ a tedy prvek a je řádu 3 v grupě G. Jelikož platí $\{a\} \cap \{b\} = 1$, kde $b \in Z$, tudíž ab = ba. Nyní máme jedinou možnost, a to zavést všechny součiny prvků a, b. Tyto prvky lze napsat ve tvaru $a^r b^s$, kde $0 \leq r \leq 2$ a $0 \leq s \leq 2$, ale jestliže devítiprvková grupa G obsahuje pouze prvky tohoto tvaru, tak prvek a komutuje s každým prvkem ve tvaru $a^r b^s$, což znamená, že $a \in Z$. Ale zde vzniká spor.

Na závěr nám tedy nezbývá než uvést, že nekomutativní grupa řádu 9 neexistuje. [3]

6.3 Nekomutativní grupy řádu pq

V následující kapitole budeme studovat nekomutativní grupy řádu pq, který je dán dvěma navzájem různými prvočísly p, q, p < q.

V první části se zaměříme grupy s řády 10, 14 a 15 a ke konci kapitoly prostudujeme grupy řádu 12, které představují zvláštní druh řádu pq, a to p^2q.

Definice 28 Sylowova p-grupa

Buď G grupa řádu $p^n \cdot m$, (m, p) = 1. Pak každou podgrupu grupy G řádu p^n nazýváme sylowovskou p-grupou grupy G. [3]

Definice 29 Konjugence

Buď G grupa, $g, h \in G$. Prvek h je konjugován s prvkem g v G, jestliže existuje prvek $x \in G$ takový, že $h = x^{-1}gx$. Obdobně podgrupy H, K grupy G jsou konjugovány v G, jestliže existuje prvek $x \in G$ tak, že $x^{-1}Hx = K$. [3]

Věta 23

Nechť G je konečná grupa řádu n a nechť p je prvočíslo, které dělí n. Potom grupa G obsahuje sylowovskou p-podgrupu.

Pro další konstrukce konečných nekomutativních grup s řádem pq budeme používat Sylowovy věty, které právě zavedeme.

1. Sylowova věta

Každá p-podgrupa H konečné grupy G je obsažena v některé sylowovské p-podgrupě grupy G. [3]

2. Sylowova věta

Každé dvě sylowovské p-podgrupy konečné grupy G jsou konjugované. [3]

3. Sylowova věta

Buď G konečná grupa a p prvočíslo dělící řád grupy G. Pak počet všech sylowovských p-podgrup grupy G dělí o (G) a je roven 1 + kp, kde k je jisté nezáporné celé číslo. [3]

Po zavedení Sylowových vět, které jsou potřebné pro další konstrukce grup řádu pq, se můžeme obrátit na praktickou stránku této kapitoly. Tudíž budeme zkoumat, jak jsme již zpočátku této kapitoly uvedli, konečné grupy řádu 10, 14 a 15. Uveďme ještě, jestliže grupa G obsahuje pouze jedinou sylowovskou p-podgrupu P, je tato p-podgrupa P podle 2. Sylowovy věty konjugována sama se sebou. Podle definice 29 to znamená, že pro každý prvek $g \in G$ platí vztah $x^{-1}Px = P$. V tomto případě je sylowovská p-podgrupa P podle věty 3 normální podgrupou grupy G. [3]

Peter Ludwig Mejdell Sylow

obrázek 5: Peter Ludwig Mejdell Sylow

Peter Ludwig Mejdell Sylow se narodil 12. prosince 1832 v dnešním Oslu a zemřel 7. září 1918. Studoval na univerzitě v Christianii (dnešní Oslo) a v roce 1853 vyhrál matematickou soutěž. V roce 1861 získal Sylow stipendium na cestování, a tak navštívil Berlín a Paříž. V Paříži se účastnil přednášek o teorii kuželoseček, racionální mechanice a o teorii omezení. V Berlíně se setkal s německým matematikem Kroneckerem a o rok později začal přednášet na univerzitě v Oslu, kde ve svých přednáškách vysvětloval algebraické rovnice matematiků Abela a Galoise. V dokumentu s názvem *„Théorémes sur les groupes do substitutions“*, který Sylow publikoval, se objevily právě jeho tři věty, které jsou v dnešní době téměř vždy používané pro studium konečných grup. Posléze se Sylow stal redaktorem časopisu *„Acta Mathematica“* a v roce 1894 mu byl udělen čestný doktorát na univerzitě v Kodani. [6]

6.3.1 Nekomutativní grupy řádu 10

Nechť existuje desetiprvková grupa G. Tato grupa G obsahuje sylowovské 5-podgrupy, kterých je díky 3. Sylowovy větě 1 + 5k, kde k je jisté nezáporné celé číslo a zároveň 1 + 5k musí dělit řád grupy G, v tomto případě je to číslo 10. Snadno nahlédneme, že jediným takovým k může být číslo 0. Což znamená, že v grupě G existuje pouze jediná sylowovská 5-podgrupa A. Ke všemu je sylowovská 5-podgrupa A pětiprvkovou cyklickou grupou s generátorem a, kde A = {a}, $a^5 = 1$ a s užitím definice 29 a věty 3 můžeme vyslovit, že A je normální podgrupou grupy G, A Δ G.

Avšak grupa G obsahuje ještě sylowovské 2-podgrupy, jichž je dle 3. Sylowovy věty 1 + 2r, kde r je opět jisté nezáporné celé číslo a zároveň vztah 1 + 2r dělí řád grupy G, tedy číslo 10. Stejně jako v předchozí sylowovské 5-podgrupě nahlédneme, že i zde může být číslo r rovno 0, ale také dle předpokladu za r lze dosadit číslo 2.

(a) r = 0

V tomto případě má grupa G pouze jedinou sylowovskou 2-podgrupu, jejímž generátorem je b, přičemž B = {b} a $b^2 = 1$. Tato sylowovská 2-podgrupa B je normální podgrupou grupy G, B Δ G. Dle věty 15, jenž nám říká, že direktní součin dvou cyklických grup s nesoudělnými řády m a n je cyklickou grupou s řádem mn. Tedy můžeme vyslovit, že direktní součin G = A x B tvoří cyklickou grupu řádu 10.

(b) r = 2

Při variantě, že číslo r se rovná dvěma, nám vzniká skutečnost, že grupa G má 5 sylowovských 2-podgrup. Jednu z těchto 5 sylowovských 2-podgrup označíme {b}, kde

$b^2 = 1$. Jelikož je sylowovská 5-podgrupa A normální podgrupou grupy G, podle věty 3, která určuje ekvivalentní podmínky definice normální podgrupy, platí $b^{-1}ab \in A$, což můžeme přepsat jako $b^{-1}ab = a^n$, pro n = 0, 1, 2, 3, 4. Potom i $a = b^{-2}ab^2 = b^{-1} \cdot b^{-1}ab \cdot b = b^{-1}a^nb =$ $= \underline{b^{-1}ab \cdot b^{-1}ab \cdot .....\cdot b^{-1}ab} = a^{n^2}$, přičemž podtržený výraz je zde uveden n-krát. Z tohoto vztahu vyplývá, že $a^1 = a^{n^2}$, to znamená $n^2 \equiv 1 \bmod 5$ a takovéto podmínce vyhovují právě čísla n = 1, n = 4.

Kdybychom uvážili, že n = 1, potom by $b^{-1}ab = a$, a při vynásobení prvkem b zleva by vznikl vztah ab = ba, což dává komutativní grupu, a to nechceme.

Tudíž musíme uvažovat n = 4. Vztahy prvků a, b, které definují tuto nekomutativní grupu jsou:

$a^5 = 1$, $b^2 = 1$, $b^{-1}ab = a^4$. Vynásobíme-li výraz $b^{-1}ab = a^4$ prvkem b zleva, dostáváme $ab = ba^4$, tedy $ba^4 = ab$. Z těchto relací, které definují nekomutativní konečnou grupu, ještě pro sestavení operační tabulky uvedeme vztahy:

$ba^3 = ba^3 \cdot a^5 = ba^4 \cdot a^4 = aba^4 = aab = a^2b$,

$ba^2 = ba^2 \cdot a^5 = ba^4 \cdot a^3 = aba^3 = aa^2b = a^3b$,

$ba = ba \cdot a^5 = ba^4 \cdot a^2 = aba^2 = aa^3b = a^4b$.

Nyní již můžeme napsat operační tabulku pro konečnou nekomutativní grupu řádu 10

	1	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
1	1	a	a^2	a^3	a^4	b	ab	a^2b	a^3b	a^4b
a	a	a^2	a^3	a^4	1	ab	a^2b	a^3b	a^4b	b
a^2	a^2	a^3	a^4	1	a	a^2b	a^3b	a^4b	b	ab
a^3	a^3	a^4	1	a	a^2	a^3b	a^4b	b	ab	a^2b
a^4	a^4	1	a	a^2	a^3	a^4b	b	ab	a^2b	a^3b
b	b	a^4b	a^3b	a^2b	ab	1	a^4	a^3	a^2	a
ab	ab	b	a^4b	a^3b	a^2b	a	1	a^4	a^3	a^2
a^2b	a^2b	ab	b	a^4b	a^3b	a^2	a	1	a^4	a^3
a^3b	a^3b	a^2b	ab	b	a^4b	a^3	a^2	a	1	a^4
a^4b	a^4b	a^3b	a^2b	ab	b	a^4	a^3	a^2	a	1

tabulka 18: Nekomutativní grupa řádu 10; $a^5 = 1$, $b^2 = 1$, $b^{-1}ab = a^4$

Na závěr bychom o konečné grupě G řádu 10 mohli říci, že existují dvě grupy G řádu 10, z nichž jedna je cyklickou grupou a druhá grupa G je grupa nekomutativní. [3]

6.3.2 Nekomutativní grupy řádu 14

Máme-li čtrnáctiprvkovou grupu G, potom tato grupa obsahuje sylowovské 7-podgrupy. Ovšem ta je pouze jedna, a to díky 3. Sylowovy větě, která říká, že počet všech sylowovských p-podgrup grupy G dělí o (G) a je roven 1 + kp, kde k je jisté nezáporné celé číslo. Aby číslo 1 + 7k dělilo číslo 14, musí se k = 0. To znamená, že v grupě G existuje pouze jediná sylowovská 7-podgrupa A, která je sedmiprvkovou cyklickou grupou s generátorem a, A = {a}, $a^7 = 1$, a zároveň A je normální podgrupa grupy G, A Δ G.

To ale není vše, neboť grupa G obsahuje i sylowovské 2-podgrupy, která je opět dle 3. Sylowovy věty jedna, když k = 0, nebo jich je sedm, když k = 3.

(a) k = 0

Zde nám vzniká fakt, že sylowovská 2-podgrupa B je pouze jedna, z čehož plyne, že jejím generátorem je prvek b, B = {b} a $b^2 = 1$ a B je normální podgrupou grupy G, B Δ G. Dle věty 15 lze rozhodnout, že direktní součin G = A x B je cyklickou grupou řádu 14.

(b) k = 3

Nyní má grupa G 7 sylowovských 2-podgrup. Jednu z nich označíme {b}, kde $b^2 = 1$. Sylowovská 7-podgrupa A je normální podgrupou grupy G, tudíž podle věty 3, můžeme napsat vztah $b^{-1}ab \in A$, neboli $b^{-1}ab = a^n$, pro n = 0, 1, 2, 3, 4, 5, 6. Stejně jako pro konečné grupy řádu 10, i zde lze odvodit, že $n^2 \equiv 1 \bmod 7$, přičemž této kongruenci vyhovují právě čísla n = 1 a n = 6.

> Skutečnost, že n = 1, udává vztah $b^{-1}ab = a$. Ale vynásobením prvkem b zleva vyjde ab = ba, což je komutativní grupa.
>
> Nezbývá nám nic jiného než číslo n = 6. Definujícími relacemi pro grupu G jsou $a^7 = 1$, $b^2 = 1$, $b^{-1}ab = a^6$. Při vynásobení výrazu $b^{-1}ab = a^6$ prvkem b zleva, dostaneme $ba^6 = ab$. Pro sestavení operační tabulky ještě uvedeme další vztahy, které plynou z úprav, a sice:
>
> $ba^5 = ba^5 \cdot a^7 = ba^6 \cdot a^6 = aba^6 = aab = a^2b$,
>
> $ba^4 = ba^4 \cdot a^7 = ba^6 \cdot a^5 = aba^5 = aa^2b = a^3b$,
>
> $ba^3 = ba^3 \cdot a^7 = ba^6 \cdot a^4 = aba^4 = aa^3b = a^4b$,

$ba^2 = ba^2 \cdot a^7 = ba^6 \cdot a^3 = aba^3 = aa^4b = a^5b,$

$ba = ba \cdot a^7 = ba^6 \cdot a^2 = aba^2 = aa^5b = a^6b.$

Nyní již můžeme sestavit operační tabulku pro konečnou nekomutativní grupu řádu 14.

	1	a	a^2	a^3	a^4	a^5	a^6	ab	a^2b	a^3b	a^4b	a^5b	a^6b
1	1	a	a^2	a^3	a^4	a^5	a^6	ab	a^2b	a^3b	a^4b	a^5b	a^6b
a	a	a^2	a^3	a^4	a^5	a^6	1	a^2b	a^3b	a^4b	a^5b	a^6b	b
a^2	a^2	a^3	a^4	a^5	a^6	1	a	a^3b	a^4b	a^5b	a^6b	b	ab
a^3	a^3	a^4	a^5	a^6	1	a	a^2	a^4b	a^5b	a^6b	b	ab	a^2b
a^4	a^4	a^5	a^6	1	a	a^2	a^3	a^5b	a^6b	b	ab	a^2b	a^3b
a^5	a^5	a^6	1	a	a^2	a^3	a^4	a^6b	b	ab	a^2b	a^3b	a^4b
a^6	a^6	1	a	a^2	a^3	a^4	a^5	b	ab	a^2b	a^3b	a^4b	a^5b
b	b	a^6b	a^5b	a^4b	a^3b	a^2b	ab	a^6	a^5	a^4	a^3	a^2	a
ab	ab	b	a^6b	a^5b	a^4b	a^3b	a^2b	1	a^6	a^5	a^4	a^3	a^2
a^2b	a^2b	ab	b	a^6b	a^5b	a^4b	a^3b	a	1	a^6	a^5	a^4	a^3
a^3b	a^3b	a^2b	ab	b	a^6b	a^5b	a^4b	a^2	a	1	a^6	a^5	a^4
a^4b	a^4b	a^3b	a^2b	ab	b	a^6b	a^5b	a^3	a^2	a	1	a^6	a^5
a^5b	a^5b	a^4b	a^3b	a^2b	ab	b	a^6b	a^4	a^3	a^2	a	1	a^6
a^6b	a^6b	a^5b	a^4b	a^3b	a^2b	ab	b	a^5	a^4	a^3	a^2	a	1

tabulka 19: Nekomutativní grupa řádu 14; $a^7 = 1, b^2 = 1, b^{-1}ab = a^6$

Závěrem lze říci, že existují dvě grupy G řádu 14, z nichž jedna je cyklická a druhá nekomutativní. [3]

6.3.3 Nekomutativní grupy řádu 15

Nechť existuje patnáctiprvková grupa G. Potom grupa G obsahuje sylowovskou 5-podgrupu, která je pouze jedna, a to díky 3. Sylowovo větě. Můžeme tedy vyslovit, že se jedná o pětiprvkovou cyklickou grupu s generátorem a, $A = \{a\}$, $a^5 = 1$, a zároveň o normální podgrupu grupy G, $A \Delta G$.

Grupa G rovněž obsahuje sylowovskou 3-podgrupu, která je taktéž pouze jedna neboť $1 + 3k$ dělí číslo 15, pouze pro $k = 0$, odtud pouze jedna sylowovská 3-podgrupa. Jedná se opět o tříprvkovou cyklickou grupu s generátorem b, $B = \{b\}$, $b^3 = 1$, která je zároveň normální podgrupou grupy G, $B \Delta G$.

Nyní tedy existují dvě cyklické grupy s řády 5 a 3. Čísla 5 a 3 jsou nesoudělná, tudíž lze podle věty 15 tvrdit, že grupa G tvoří cyklickou grupu řádu 15.

Závěrem lze říci, že neexistuje nekomutativní grupa řádu 15. [3]

6.3.4 Nekomutativní grupy řádu 12

Na závěr této práce jsme si nechali nekomutativní grupy řádu 12, poněvadž se jedná o zvláštní druh řádu pq, a to p^2q. Nezapomeneme, že čísla p a q jsou navzájem různá prvočísla, kde $p < q$.

Tato grupa G řádu 12 obsahuje sylowovské 3-podgrupy. Snadno můžeme nahlédnout, že pomocí 3. Sylowovy věty, je tato sylowovská 3-podgrupa právě jedna, a to normální, pro $k = 0$. Nebo existují čtyři sylowovské 3-podgrupy, které jsou navzájem konjugované, a to pro $k = 1$. Dále grupa G také obsahuje sylowovské 2-podgrupy s řádem 4. S použitím 3. Sylowovy věty snadno zjistíme, že tato sylowovská 2-podgrupa je právě jedna, a to normální, nebo jsou tyto sylowovské 2-podgrupy tři, které jsou navzájem konjugované.

Následně vyčteme případy, které mohou nastat:

(1) Jestliže existuje jediná sylowovská 3-podgrupa A a zároveň existuje jediná sylowovská 2-podgrupa B řádu 4, potom můžeme dle věty 15 rozhodnout, že direktní součin $G = A \times B$ tvoří komutativní grupu řádu 12.

(2) Ve druhém případě budeme předpokládat, že grupa G obsahuje 4 sylowovské 3-podgrupy a k tomu ještě 3 sylowovské 2-podgrupy řádu 4. Ovšem tato možnost nenastane, neboť grupa G má pouze 12 prvků a s tímto předpokladem by vzniklo prvků 18, což je spor.

(3) Nyní nastává krok, kdy existuje jediná sylowovská 3-podgrupa $A = \{a\}$ a zároveň 3 sylowovské 2-podgrupy a jednu z těchto 3 sylowovských 2-podgrup označíme B.

(a) Budeme uvažovat, že B je cyklická grupa řádu 4, kde B = {b} a $b^4 = 1$. S ohledem na to, že A je normální podgrupou grupy G, můžeme podle věty 3 napsat $b^{-1}ab = a^n$, kde n = 0, 1, 2. Rovnosti $n^2 \equiv 1 \bmod 3$ vyhovují čísla n = 1 a n = 2. Pro n = 1 však vznikne po vynásobení vztahu $b^{-1}ab = a$ prvkem b zleva rovnost ab = ba, což je komutativní grupa.

Zbývá tedy vyřešit n = 2. Nastává situace, kdy $b^{-1}ab = a^2$. Definujícími relacemi pro grupu G jsou $a^3 = 1$, $b^4 = 1$, $ba^2 = ab$. Pro konstrukci operační tabulky vyjádříme ještě ostatní relace typu $b^x a^y = a^k b^l$:

$ba = ba \cdot a^3 = ba^2 \cdot a^2 = aba^2 = aab = a^2b$,

$b^2a = b \cdot ba = ba^2b = abb = ab^2$,

$b^2a^2 = b \cdot ba^2 = bab = a^2bb = a^2b^2$,

$b^3a = b \cdot b^2a = bab^2 = a^2bb^2 = a^2b^3$,

$b^3a^2 = b \cdot b^2a^2 = ba^2b^2 = abb^2 = ab^3$.

Nyní sestrojíme operační tabulku.

	1	a	a^2	b	b^2	b^3	ab	ab^2	ab^3	a^2b	a^2b^2	a^2b^3
1	1	a	a^2	b	b^2	b^3	ab	ab^2	ab^3	a^2b	a^2b^2	a^2b^3
a	a	a^2	1	ab	ab^2	ab^3	a^2b	a^2b^2	a^2b^3	b	b^2	b^3
a^2	a^2	1	a	a^2b	a^2b^2	a^2b^3	b	b^2	b^3	ab	ab^2	ab^3
b	b	a^2b	ab	b^2	b^3	1	a^2b^2	a^2b^3	a^2	ab^2	ab^3	a
b^2	b^2	ab^2	a^2b^2	b^3	b	b	ab^3	a	ab	a^2b^3	a^2	a^2b
b^3	b^3	a^2b^3	ab^3	1	b	b^2	a^2	a^2b	a^2b^2	a	ab	ab^2
ab	ab	b	a^2b	ab^2	ab^2	a	b^2	b^3	1	a^2b^2	a^2b^3	a^2
ab^2	ab^2	a^2b^2	b^2	ab^2	a	ab	a^2b^3	a^2	a^2b	b^3	1	b
ab^3	ab^3	b^3	a^2b^3	a	ab	ab^2	1	b	b^2	a^2	a^2b	a^2b^2
a^2b	a^2b	ab	b	a^2b^2	a^2b^3	a^2	ab^2	ab^3	a	b^2	b^3	1
a^2b^2	a^2b^2	b^2	ab^2	a^2b^3	a^2	a^2b	b^3	1	b	ab^3	a	ab
a^2b^3	a^2b^3	ab^3	b^3	a^2	a^2b	a^2b^2	a	ab	ab^2	1	b	b^2

tabulka 20: Nekomutativní grupa řádu 12; $a^3 = 1$, $b^4 = 1$, $b^{-1}ab = a^2$

Vznikla nám tedy nekomutativní grupa řádu 12.

(b) Následně budeme uvažovat, že B je Kleinova čtyřgrupa s generátory b, c, které splňují relace $b^2 = 1$, $c^2 = 1$ a $bc = cb$. Jelikož je A normální podgrupou grupy G, tudíž dle věty 3 můžeme napsat $b^{-1}ab = a^n$, pro n = 0, 1, 2, a stejně tak $c^{-1}ac = a^m$, pro m = 0, 1, 2. Rovnosti $n^2 \equiv 1 \bmod 3$, resp. $m^2 \equiv 1 \bmod 3$, vyhovují čísla n = 1, n = 2, resp. m = 1, m = 2, z čehož mohou nastat následující možnosti:

1. n = m = 1, ovšem grupa G by byla komutativní, neboť by nastala rovnost ab = ba, resp. ac = ca.

2. n = 1, m = 2, popř. n = 2, m = 1, po přeznačení prvků b a c se ukazuje, že obě tyto možnosti jsou stejné. Definující relace $a^3 = 1$, $b^2 = c^2 = 1$, $bc = cb$, $b^{-1}ab = a$, $c^{-1}ac = a^2$, popř. $b^{-1}ab = a^2$, $c^{-1}ac = a$, určují další nekomutativní grupu G řádu 12.

3. n = m = 2, znamená, že se jedná opět o nekomutativní grupu G řádu 12 s definujícími relacemi $a^3 = 1$, $b^2 = c^2 = 1$, $bc = cb$, $b^{-1}ab = a^2$, $c^{-1}ac = a^2$.

(4) V posledním případě budeme předpokládat, že existuje jedna sylowovská 2-podgrupa E řádu 4 a zároveň 4 sylowovské 3-podgrupy, z nichž jednu označíme F.

(a) Budeme uvažovat, že E je cyklická grupa řádu 4, E = {e}, kde $e^4 = 1$ a F = {f}, kde $f^3 = 1$ je jedna ze 4 sylowovských 3-podgrup. E je normální podgrupa grupy G potom podle věty 3 můžeme napsat $f^{-1}ef = e^n$, kde n = 0, 1, 2, 3. Rovnosti $n^3 \equiv 1 \bmod 4$ odpovídá pouze číslo n = 1, avšak jednalo by se o komutativní grupu.

(b) Nyní budeme uvažovat, že E je Kleinova čtyřgrupa s generátory d, e, kde $d^2 = e^2 = 1$ a zároveň de = ed, E Δ G. Nechť F = {f}, kde $f^3 = 1$ je jedna ze 4 sylowovských 3-podgrup, potom dle věty 3 platí $f^{-1}df = d^m e^n$ a $f^{-1}ef = d^r e^s$, kde čísla m, n, r, s jsou buďto 0 či 1, ale nemohou být m = n = 0, resp. r = s = 0, protože to vede ke sporu. Možnosti, které mohou nastat vyčteme:

- m = n = 1, r = s = 1 zřejmě nenastane, neboť by musely platit rovnosti $f^{-1}df = de$, $f^{-1}ef = de$, z čehož plyne, že $f^{-1}df = f^{-1}ef$, neboli d = e, a to je spor.
- m = n = 1, r = 1, s = 0, tzn. $f^{-1}df = de$, $f^{-1}ef = d$, což skutečně nastat může, neboť $e = f^{-3}ef^{3} = f^{-1}(f^{-1}(f^{-1}ef)f)f = f^{-1}(f^{-1}df)f = f^{-1}def = f^{-1}df \cdot f^{-1}ef = ded = e$.
- m = n = 1, r = 0, s = 1, tzn. $f^{-1}df = de$, $f^{-1}ef = e$, tato možnost nenastane, neboť $d = f^{-3}df^3 = f^{-1}(f^{-1}(f^{-1}df)f)f = f^{-1}(f^{-1}def)f = f^{-1}(f^{-1}df \cdot f^{-1}ef)f = f^{-1}deef = f^{-1}df = de$, ale $d \neq de$.
- m = 1, n = 0, r = s = 1, což udává relace $f^{-1}df = d$, $f^{-1}ef = de$, které opět nenastanou, $e = f^{-3}ef^3 = f^{-1}(f^{-1}(f^{-1}ef)f)f = f^{-1}(f^{-1}def)f = f^{-1}(f^{-1}df \cdot f^{-1}ef)f = f^{-1}ddef = f^{-1}ef = de$, ale $e \neq de$.
- m = 1, n = 0, r = 1, s = 0 zřejmě nenastane, muselo by platit $f^{-1}df = d$, $f^{-1}ef = d$, ale $d \neq e$.
- m = 1, n = 0, r = 0, s = 1, tzn. $f^{-1}df = d$, $f^{-1}ef = e$, potom ale df = fd, ef = fe a zároveň z předpokladu víme, že de = ed, tudíž se jedná o komutativní grupu.
- m = 0, n = 1, r = s = 1, tzn. $f^{-1}df = e$, $f^{-1}ef = de$, při přeznačení prvků d, e nastává obdobná situace jako u druhé odrážky.
- m = 0, n = 1, r = 1, s = 0, tzn. $f^{-1}df = e$, $f^{-1}ef = d$, což nemůže nastat, $d = f^{-3}df^3 = f^{-1}(f^{-1}(f^{-1}df)f)f = f^{-1}(f^{-1}ef)f = f^{-1}df = e$, ale $d \neq e$.

- m = 0, n = 1, r = 0, s = 1, tzn. $f^{-1}df = e$, $f^{-1}ef = e$, snadno nahlédneme, že ani tato možnost nenastane, neboť $d \neq e$.

Z tohoto výčtu jsme zjistili, že existují další dvě nekomutativní grupy řádu 12, a to zadané relacemi $d^2 = e^2 = 1$, $de = ed$, $f^3 = 1$, $f^{-1}df = de$, $f^{-1}ef = d$, resp. $f^{-1}df = e$, $f^{-1}ef = de$. [3]

Závěr

Ve své práci jsem se snažila zachytit všechny znalosti, které jsem získala studiem konečných grup na základě uvedené literatury. Cílem této práce bylo seznámit čtenáře s teorií grup a větami k tomuto tématu potřebné. Pomocí těchto vět již bylo snadné nalézt relace, jenž určují konečné grupy.

Se studiem grup se můžeme setkat především v přírodních vědách, jako jsou např. fyzika či chemie. Tyto disciplíny využívají teorii grup pro své další účely, přičemž v chemii se teorie grup používá pro popis krystalových mřížek v krystalografii, fyzika teorii grup využívá především v částicové či jaderné fyzice.

Seznam literatury

[1] Burian, K., Libicher, J.: *Algebra 1*. 2. vyd. Ostrava: Pedagogická fakulta v Ostravě, 1976, str. 54 – 65.

[2] Hora, J.: *Algebra 1*. 1. vyd. Plzeň: Pedagogická fakulta v Plzni, 1991, str. 13 – 16, 21, 35 – 40. ISBN 80-7043-030-3.

[3] Hora, J.: *Konečné grupy malých řádů*. In: Sborník PdF Plzeň Matematika V., str. 56 – 73, 1989.

[4] Elementární algebra [online]/ Binární operace. Jejich vlastnosti. Algebraické struktury a jejich zobrazení.

http://www.kmt.zcu.cz/subjects/ela.html

[5] **Full MacTutor Biography** [online]/ autor John J O´ Connor a Edmund F Robertson// Full MacTutor Biography. – Niels Henrik Abel, červenec 2008.

http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Abel.html

[6] **Full MacTutor Biography** [online]/ autor John J O´ Connor a Edmund F Robertson// Full MacTutor Biography. – Peter Ludwig Mejdell Sylow, červenec 2008.

http://www-history.mcs.st-andrews.ac.uk/Mathematicians/Sylow.html

[7] Základy teorie grup [online]/ autor Martin Kuřil// Základy teorie grup.
http://katmatprf.ujepurkyne.com/materialy/kuril_grupy.pdf

[8] Grupa [online]

http://cs.wikipedia.org/wiki/Grupa

Seznam tabulek

Seznam obrázků

Resumé

The topic of this Bachelor thesis is “Final groups of small orders ”. The thesis is focused on the group theory and its terminology. Individual examples of the terms will help the reader to understand the problems of this topic as well as the solution procedures, which are determined by mathematical sentences. These procedures are necessary to determine whether the groups are either commutative or non commutative. In this thesis there are mentioned operational tables of individual final groups. Firstly the thesis deals with the processing of final commutative groups and consequently it focuses on non commutative groups.