ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

OKRUHY S MALÝM POČTEM PRVKŮ

DIPLOMOVÁ PRÁCE

Bc. Michaela Neužilová
Učitelství pro základní školy, obor Ma-CH

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

Plzeň 2018

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

Plzeň, 28. června 2018

.....

vlastnoruční podpis

Děkuji vedoucímu mé diplomové práce doc. RNDr. Jaroslavu Horovi, CSc. za odborné vedení, cenné rady a čas, který mi věnoval.

Zde se nachází originál zadání diplomové práce

Obsah

Úvod

Jak již z názvu vyplývá, tato práce se zaměřuje na okruhy s malým počtem prvků. Diplomová práce zpracovává téma týkající se konečných algebraických struktur (konkrétně okruhů malých řádů, ale je zde obsaženo i téma týkající se grup). Teprve na vysoké školy se studenti v hodinách (seminářích a přednáškách) seznamují podrobně s různými algebraickými strukturami buďto s jednou nebo i se dvěma operacemi. Je jasné, že teorie grup, okruhů a dalších algebraických struktur je budována od jednodušších po složitější struktury. I z toho plyne důležitost konečných struktur malých řádů. Stejně tak je jasné, že tyto struktury slouží studentům k pochopení a získání představy o probírané látce. Znalost těchto příkladů pomáhá studentům získat konkrétní představu o probírané teorii a zároveň jsou studenti vybaveni jednoduchými příklady probíraných struktur. Ty mohou studentům pomoci pochopit definice a věty, které budou při rozvíjení teorie následovat. Ale je pravdou, že s některými strukturami se mohou setkat již žáci na základní škole, aniž by věděli, že s něčím takovým pracují.

Tato práce navazuje na znalosti, které studenti získají z hodin algebry a shrnuje základní vlastnosti konečných grup malých řádů a konečných okruhů malých řádů. Zároveň se v teorii grup seznámíme s Sylowovými větami, které jsou velmi důležité.

Veškeré definice a věty jsem převzala doslovně nebo s menšími úpravami tak, aby odpovídaly pojmům teorie grup a okruhů s malým počtem prvků, ze zdrojů, které jsou uvedeny v závěru práce v seznamu použité literatury.

Historické poznámky o vývoji teorie grup

První podněty ke studiu teorie grup jsou z doby, kdy byla intenzivně studována řešitelnost obecných algebraických rovnic n-tého stupně. Mezi první matematiky, kteří se zabývali studiem grup substitucí (v dnešní terminologii grupy permutací kořenů), byli Lagrange, Ruffini a Cauchy. Klasické strukturální věty byly zcela pochopitelně objeveny až později.

Na jaře roku 1872 norský matematik M. L. Sylow publikoval v „Matematische Annalen“ článek, který byl nazvaný „Theoremes sur les groupes de substitution“, který obsahovala dnešní „Sylowovy věty“. Nový důkaz těchto vět nalezl v roce 1877 G. Frobenius. „Hlavní větu“ o konečných Abelových grupách, které jsou direktními součty cyklických grup (včetně jednoznačných faktorů) dokázali G. Frobenius a L. Stickelberger v roce 1879. Řadu klasických výsledků pak získal i O. Hölder (například článek „Die Gruppen der Ordnungen p^3, pq^2, p^4“ v „Matematische Annalen“ v roce 1893). Velmi dlouhou dobu však byly studovány pouze konečné grupy, anebo alespoň třídy grup s jistou podmínkou konečnosti (tzv. konečně generované grupy apod.). Zřejmě prvním, kdo opustil i tyto podmínky a otevřel studium nekonečných grup v plné obecnosti, byl O. J. Schmidt, což byl zakladatel ruské školy teorie grup (kniha „Abstraktní teorie grup“, Kyjev 1916).

Základní pojmy teorie grup

Definice 1

Algebraickou strukturu $(\mathrm{M},\otimes)$ nazýváme grupou právě tehdy, když je tato struktura asociativní, má jednotkový prvek a k jakémukoli prvku z *M* existuje v *M* inverzní prvek.

Definice 2

Algebraickou strukturu $\mathrm{G}_1=(\mathrm{M}_1,\otimes_1)$ nazýváme podgrupou grupy $\mathrm{G}=(\mathrm{M},\otimes)$ právě tehdy, když $\emptyset\neq M_1\subset M, 1\in M$, kde 1 označuje jednotkový prvek grupy *G*, a dále $(\forall a,b\in M_1)\ a\otimes_1 b\in M_1,\ a^{-1}\in M_1$. (Značíme $G_1\leq G$).

Věta o charakterizaci podgrupy

Mějme grupu $\mathrm{G}=(\mathrm{M},\otimes)$ a $\varnothing \neq M_1 \subseteq M$, potom $\mathrm{G}_1=(\mathrm{M}_1,\otimes_1)$ je podgrupou G právě tehdy, když:

a) $\forall k \in M_1 : k^{-1} \in M_1$

b) $\forall k_1, k_2 \in M_1 : k_1 \otimes_1 k_2 \in M_1$

Je známo, že obě tyto podmínky lze spojit do jedné, a to: $\forall k_1, k_2 \in M_1 : k_1 \otimes_1 k_2^{-1} \in M_1$.

Definice 3

Nechť H je podgrupou grupy G, $k \in G$. Potom množinu $kH=\{kh, h \in H\}$ (respektive $Hk=\{hk, h \in H\}$) nazveme levou (respektive pravou) třídou grupy G podle podgrupy H, která je určená prvkem k.

Příklad 1

Máme grupu G shodností v rovině reprodukujících rovnostranný trojúhelník ABC (to znamená $G=\left(\left\{I, O_1, O_2, O_3, \mathrm{R}, \mathrm{R}^2\right\}, \circ\right)$. Podgrupu H označme jako rotaci $H=\left(\left\{I, R, R^2\right\}, \circ\right)$. Utvořme všechny levé třídy grupy G podle podgrupy H.

Řešení:

Máme

$$IH=\left\{I, R, R^2\right\} \qquad O_1H=\left\{O_1, O_2, O_3\right\}$$

$$RH=\left\{R, R^2, \mathrm{I}\right\} \qquad O_2H=\left\{O_2, O_1, O_3\right\}$$

$$R^2H=\left\{R^2, I, R\right\} \qquad O_3H=\left\{O_3, O_2, O_1\right\}$$

Ukazuje se, že každé dvě levé (respektive pravé) třídy se buď rovnají, nebo jsou disjunktní. Vznikl nám tedy rozklad množiny $\left\{I, O_1, O_2, O_3, \mathrm{R}, \mathrm{R}^2\right\}$ na třídy. To platí obecně.

Věta 1

Pro každé dvě levé třídy grupy G podle podgrupy H platí, že se buď rovnají, nebo jsou disjunktní.

Důkaz

Mějme dvě třídy kH, lH, které nejsou disjunktní. Existuje tedy prvek a, který má vlastnost $a \in kH \cap lH$. Dále mějme $y \in kH$, který je libovolný. Je $y = kh$ pro jistý $h \in H$, obdobně i $a = kh_1 = lh_2$ pro jisté prvky $h_1, h_2 \in H$. Dále také máme $k = lh_2 h_1^{-1} \cdot h = l \cdot \left(h_2 \cdot h_1^{-1} \cdot h \right) \in lH$, to znamená, že $kH \subseteq lH$. Podobným způsobem se ukáže inkluze $kH \supseteq lH$, proto tedy platí $kH = lH$.

Důkaz obdobné věty o pravých třídách je analogický, proto ho nebudeme rozebírat. Ještě si všimněme, že pokud $h \in H$, potom $hH = H$. Podgrupa H představuje jednu z levých (respektive pravých) tříd grupy G podle H.

Věta 2

Mohutnost množiny *R* všech navzájem různých levých tříd grupy *G* podle podgrupy *H* je rovna mohutnosti množiny *S* všech navzájem různých pravých tříd grupy *G* podle podgrupy *H*.

Důkaz

Definujme zobrazení $\varphi R \to S$ tak, že pro každé $g \in G$ položíme $\varphi(gH) = Hg^{-1}$. Pro prvky $r, s \in G$ platí rovnost $rH = sH$ právě tehdy, když $s^{-1}r \in H$, neboli právě tehdy, když $s^{-1}(r^{-1})^{-1} \in H$, a tedy právě když $Hr^{-1} = Hs^{-1}$. To znamená, že φ je opravdu korektně definované zobrazení, ale také to, že φ je injekce. Protože φ je zřejmě projektivní, tak je věta dokázána.

Definice 4

Mohutnost množiny všech různých levých (popřípadě pravých) tříd grupy *G* podle podgrupy *H* je nazývána jako index podgrupy *H* v grupě *G* a je značena $G = Z_2 \times Z_5 \cong Z_{10}$.

Definice 5

Je-li $\left[G : H \right] \leq \chi_0$, řekneme, že *H* je konečného indexu v *G*. V opačném případě jde o nekonečný index v *G*.

Definice 6

Zobrazení $\varphi: H \to G$ nazveme homomorfismem grup $(H,\oplus)$, $(G,\otimes)$ právě tehdy, když platí: $(\forall r,s \in H): \varphi(r \oplus s) = \varphi(r) \oplus \varphi(s)$.

Definice 7

Pokud je $\varphi: (H,\oplus) \to \varphi(\mathrm{G},\otimes)$ homomorfismem grup a je-li zároveň φ bijekce, potom zobrazení φ nazýváme izomorfismus a říkáme, že grupa $(H,\oplus)$ je izomorfní s grupou $(G,\otimes)$. (Píšeme $H \cong G$).

Lagrangeova věta

Lagrangeova[1] věta přesně a jasně vymezuje řády podgrup, které jsou možné.

Věta 3

Je-li H podgrupou konečné grupy G, potom platí, že $o(G) = o(H) \cdot [G:H]$. Přičemž $o(\mathrm{G})$ a $o(H)$ značí řád grupy G a H.

Důsledek Lagrangeovy věty

Buď G konečná grupa, $g \in$ G. Potom $o(g)$ dělí $o(\mathrm{G})$, což znamená, že řád prvku g dělí řád grupy G.

Cyklické grupy

Definice 8

Mějme M jako podmnožinu grupy G. Průnik všech podgrup grupy G, které obsahují množinu M, nazveme podgrupou generovanou množinou M a označíme ji {M}. Pokud $\{M\} = G$, potom M nazveme množinou generátorů grupy G. Grupu G, která je generovaná množinou $\{g\}$ nazýváme cyklická grupa. Píšeme $G = \langle g \rangle$.

[1] Joseph-Louis Lagrange (původním jménem Giuseppe Lodovico Lagrangia) byl francouzský matematik a astronom (ovšem italského původu). Zasloužil se o významné rozvinutí matematické analýzy, teorie čísel, klasické a nebeské mechaniky.

Věta 4

Nechť M je podmnožina grupy G. Je-li $M = \varnothing$, potom $\{M\} = \{e\}$ (to znamená, že neprázdná množina generuje triviální podgrupu). Je-li ale $M \neq \varnothing$, potom $\{M\} = \left\{ m_1^{e_1} \cdot m_2^{e_2} \cdot \ldots \cdot m_n^{e_n}; m_i \notin M, e_i \in Z, i = 1, 2, \ldots, n \in N \right\}$. (Neprázdná množina generátorů M nageneruje tedy množinu „slov“ konečné délky tvořených celočíselnými mocninami prvků množiny M.

Důkaz

V první části je {M}průnik všech podgrup, které obsahují $\varnothing$, to znamená, že je to průnik všech podgrup grupy G. Je tedy zřejmé, že je tento průnik jednotkovou podgrupou $(\{e\}, \cdot)$.

Ve druhé části označíme $H = \left\{ m_1^{e_1} \cdot \ldots \cdot m_n^{e_n}; m_i \in M, e_i \in Z, n \in N \right\}$. Nechť A je podgrupa grupy G, která obsahuje množinu M, pak A nutně musí obsahovat množinu „slov“ H, tzn. $H \subseteq A$ a také $H \subseteq \{M\}$. Pokud bychom ještě dokázali inkluzi $H \supseteq \{M\}$, tak by platilo $\{M\} = H$ a bylo by vše vyřešeno. Samotná množina M je ale podmnožinou množiny „slov“ H (smíme psát ″slova″ m_i délky 1 s exponentem l, $m_i \in M$). Dále také ukažme, že množina H s operací $\cdot$ je podgrupou grupy G.

Jsou-li $x = m_1^{e_1} \cdot m_2^{e_2} \cdot \ldots \cdot m_k^{e_k}$ a $y = m_1'^{f_1} \cdot m_2'^{f_2} \cdot \ldots \cdot m_l'^{f_l}$ dva prvky z H, potom $y^{-1} = m_l'^{-f_l} \cdot \ldots \cdot m_1'^{-f_l}$, a $x \cdot y^{-1} = m_1^{e_1} \cdot \ldots \cdot m_k^{e_k} \cdot m_l'^{-f_l} \cdot \ldots m_1'^{-f_1}$, což je také prvek množiny H, to znamená „slovo“ konečné délky utvořené z mocnin prvků množiny M s celočíselnými exponenty. Je tedy H grupa, která obsahuje množinu M, proto H obsahuje {M}, $H \supseteq \{M\}$. Tím je důkaz rovnosti $H = \{M\}$ hotový.

Z věty 2 plyne, že se tedy jedná o grupy, které jsou tvořené celočíselnými mocninami generátoru g.

Lemma 1

Nechť G je grupa, $x \in G$. Potom $(x^{-1})^n = (x^n)^{-1}$ pro každé přirozené číslo n. Prvek $(x^{-1})^n$ budeme značit x^{-n}.

Důkaz

Platí $(x^{-1})^n \cdot x^n = x^n \cdot (x^{-1})^n = e$. Proto $(x^{-1})^n = (x^n)^{-1}$ podle věty o inverzním prvku.

Věta 5

Nechť $\langle a \rangle$ je cyklická grupa. Potom všechny celočíselné mocniny prvku a jsou navzájem různé a cyklická grupa $\langle a \rangle$ je nekonečná, anebo existuje přirozené číslo n takové, že bude platit $\langle a \rangle = \{a, a^2, \ldots, a^n = e\}$. A přitom platí $a^m = e$ právě tehdy, když $n \mid m$.

Příklad 2

V množině komplexních čísel $\mathbb{C}$ řešte rovnici $x^4 = 1$. Ukažte, že množina všech kořenů této rovnice spolu s operací násobení komplexních čísel tvoří cyklickou grupu.

Řešení: Tato rovnice ($x^4 = 1$) má v množině komplexních čísel $\mathbb{C}$ právě 4 kořeny (1, -1, i, -i). Dostaneme tedy čtyřprvkovou grupu

.	**1**	**i**	**-1**	**-i**
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Z této tabulky snadno zjistíme, že jde o grupu cyklickou, protože generátory jsou i (respektive –i). Například $(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$. Tato cyklická grupa obsahuje také kromě nevlastních podgrup i cyklickou podgrupu řádu 2, generovanou prvkem -1.

Věta 6

Nechť $\langle a \rangle$ je konečná cyklická grupa řádu n. Potom $\langle a^m \rangle = \langle a \rangle$ právě tehdy, když platí $(m,n)=1$. (Pro připomenutí symbolem $(m,n)=1$ je označován největší společný dělitel čísel m,n)

Příklad 3

Určete počet generátorů cyklické grupy $\langle a \rangle$ řádu 10.

Řešení:

V množině čísel $\{1,2,3,4,5,6,7,8,9,10\}$ jsou čtyři čísla, která nejsou soudělná s číslem 10 (tzn. že jejich největší společný dělitel je 1). Jsou to čísla 1, 3, 7, 9. Je $\varphi(10)=4$ a generátory grupy $\langle a \rangle$ jsou v tomto případě prvky a, a^3, a^7, a^9.

Dále si ještě povšimněme, jak vypadá podgrupa grupy $\langle a \rangle$ generovaná kupříkladu prvkem a^2. To znamená $\left(a^2\right)^2 = a^4$, $\left(a^2\right)^3 = a^6$, $\left(a^2\right)^4 = a^8$, $\left(a^2\right)^5 = a^{10} = e$. Z toho vidíme, že $\langle a^2 \rangle = \{a^2, a^4, a^6, a^8, e\}$ je cyklická podgrupa řádu 5 grupy $\langle a \rangle$. Stejným způsobem můžeme dále zjistit, že $\langle a^5 \rangle = \{a^5, a^{10} = e\}$ je také cyklickou podgrupou řádu 2 grupy $\langle a \rangle$.

Tvrzení

1) Každá podgrupa cyklické grupy je také cyklická.
2) Pokud je $\langle a \rangle$ konečná cyklická grupa řádu n a d přirozené číslo, které dělí n, $n = d \cdot m$, potom $\langle a \rangle$ obsahuje jednu jedinou podgrupu řádu d, a to $\langle a^m \rangle$.

Z tohoto tvrzení tedy vyplývá, že konečná cyklická grupa $\langle a \rangle$ řádu n má právě tolik rozlišných podgrup, kolik přirozených dělitelů má číslo n.

Grupy prvočíselných řádů

Věta 7

Každá grupa prvočíselného řádu je cyklická.

Důkaz

Buď G grupa prvočíselného řádu p a $g \neq 1$ její libovolný prvek. Podle důsledku Lagrangeovy věty dělí řád prvku g prvočíslo p, a tedy řád prvku g je roven p (protože p je prvočíslo a je tedy dělitelné pouze jedničkou a samo sebou). Potom ovšem platí $G = \{g\}$.

Věta 8

Grupa G nemá žádné vlastní podgrupy právě tehdy, pokud je grupou prvočíselného řádu.

Důkaz

Mějme G (grupa prvočíselného řádu) a $1 \neq H \leq G$ nechť je podgrupou grupy G. Dále buď $1 \neq h \in H$ libovolný prvek. Dle důkazu předchozí věty platí, že $G = \{h\} \leq H$, takže je tedy zřejmé, že $G = H$. Grupa tedy nemá vlastní podgrupy. Tím je dokázáno, že má-li grupa prvočíselný řád, nemá vlastní podgrupy, jde tedy o implikaci $\Leftarrow$. Teď zbývá dokázat implikaci $\Rightarrow$, tedy to, že z neexistence vlastních podgrup vyplývá prvočíselnost grupy. Nechť tedy G nemá žádné vlastní podgrupy. Je-li $1 \neq g \in G$ libovolný prvek, je tedy $G = \{g\}$ a G je cyklická. Vzhledem k tomu, že nekonečná cyklická grupa má dokonce nekonečně mnoho vlastních podgrup, musí tedy být G konečnou cyklickou grupou. Kdyby byl řád grupy G složeným číslem a d by byl vlastní dělitel $o(G)$, obsahovala by grupa G vlastní podgrupu $\{g^d\}$. Z toho plyne, že je tedy cyklickou grupou prvočíselného řádu. Tím jsme dokázali celou ekvivalenci a důkaz věty je tedy hotov.

Definice 9

Podgrupu $G_1 = (M_1, \otimes)$ grupy $G = (M, \otimes)$ nazveme normální podgrupou, pokud $(\forall u \in M)(\forall v \in M_1) u^{-1} \otimes v \otimes u \in M_1$. (Značíme $G_1 \Delta G$).

POZNÁMKA: Každá podgrupa komutativní grupy je normální podgrupou.

1 a G jsou vždy normální podgrupy grupy G.

Je- li $[G:H]=2$, potom je $H \Delta G$.

Definice 10

Grupu G nazveme jednoduchou grupou, pokud nemá vlastní normální podgrupy.

V teorii grup mají jednoduché grupy velmi důležitou roli. Z předchozích vět a definic je jasné, že jsme získali popis všech grup řádů 2, 3, 5, 7, 11, 13. Pro lepší představu je vhodné uvést některé operační tabulky.

G	**1**	**u**
1	1	u
u	u	1

Tabulka 1: Cyklická grupa řádu 2

H	**1**	**u**	**u^2**
1	1	u	u^2
u	u	u^2	1
u^2	u^2	1	u

Tabulka 2: Cyklická grupa řádu 3

I	**1**	**u**	**u^2**	**u^3**	**u^4**
1	1	u	u^2	u^3	u^4
u	u	u^2	u^3	u^4	1
u^2	u^2	u^3	u^4	1	u
u^3	u^3	u^4	1	u	u^2
u^4	u^4	1	u	u^2	u^3

Tabulka 3: Cyklická grupa řádu 5

První tabulka představuje prvočíselnou cyklickou grupu *G* řádu dva, druhá tabulka představuje prvočíselnou cyklickou grupu *H* řádu tři a třetí tabulka představuje prvočíselnou cyklickou grupu *I* řádu pět.

Z těchto tabulek lze vyčíst některé vlastnosti popisované struktury. Na první pohled je jasné, že struktury jsou komutativní, protože tabulky jsou souměrné podle diagonály. Dále jsou také ekvivalentní, že prvky označené jako 1, jsou opravdu jednotkové prvky, pro které platí vždy předpis $u^k = 1$, kde *k* je řád prvočíselné cyklické grupy. I v jiném značení lze velmi jednoduše rozlišit, který prvek je jednotkový (neutrální) a to tak, že v řádku (popřípadě sloupci), v jehož záhlaví je tento prvek, se reprodukuje celé záhlaví tabulky.

Další cyklické grupy prvočíselných řádů už nebudeme popisovat tabulkou, protože tyto tabulky jsou analogické s uvedenými a konstruují se zcela stejným způsobem, liší se pouze počtu řádků podle toho, o jakou grupu se jedná. Dále také proto, že tyto tabulky už by byly velmi obsáhlé.

Grupy řádu 4

Při studiu grup řádu 4 a později řádu 8 využijeme následující lemma.

Lemma 2

Buď *G* taková grupa, ve které pro každý prvek *u* platí $u^2 = 1$, potom *G* je Abelova (komutativní) grupa.

Důkaz

Nechť *u, v* jsou dva libovolné prvky z *G*. Je $1 = (uv)^2 = uvuv$, vynásobíme-li prvkem vu zleva, dostaneme rovnost $vu = vuuvuv$. Vzhledem k tomu, že $u^2 = 1$, dostáváme $vu = v \cdot 1 \cdot vuv$, jednička je neutrální prvek, a tedy $vu = vvuv$ a jelikož víme, že $v^2 = 1$, dostaneme rovnost $vu = uv$ a komutativnost je ověřena.

Grupy řádu 4 lze rozdělit do dvou skupin a to podle toho, se kterou ze dvou základních grup jsou izomorfní.

H	**1**	**u**	**u^2**	**u^3**
1	1	u	u^2	u^3
u	u	u^2	u^3	1
u^2	u^2	u^3	1	u
u^3	u^3	1	u	u^2

První skupinu tvoří grupy, ve kterých existuje prvek řádu čtyři. Tyto grupy jsou cyklické grupy řádu 4 a lze je popsat touto operační tabulkou. Jsou tedy izomorfní s grupou *H*.

G	**1**	**u**	**v**	**uv**
1	1	u	v	uv
u	u	1	uv	v
v	v	uv	1	u
uv	uv	v	u	1

Pokud grupa *G* neobsahuje prvek řádu čtyři, potom podle důsledku Lagrangeovy věty mají všechny nejednotkové prvky řád dva a podle lemmatu 2 je *G* komutativní. Označíme-li *u, v* dva nejednotkové prvky z *G*, $u \neq v$, potom v *G* musí platit $u^2 = v^2 = 1$, $uv = vu$. Tyto relace nám dovolují napsat operační tabulku. Touto Cayleyho tabulkou je dána tzv. Kleinova čtyřgrupa. Díky předpokladu, že v *G* neexistuje prvek řádu 4, je jasné, že tato grupa není izomorfní se čtyřprvkovou cyklickou grupou.

Až na izomorfismus tedy existují dvě grupy řádu 4.

Grupy řádu 6

K teorii grup řádu šest budeme přistupovat podobně jako u grup řádu čtyři.

I	**1**	**u**	**u^2**	**u^3**	**u^4**	**u^5**
1	1	u	u^2	u^3	u^4	u^5
u	u	u^2	u^3	u^4	u^5	1
u^2	u^2	u^3	u^4	u^5	1	u
u^3	u^3	u^4	u^5	1	u	u^2
u^4	u^4	u^5	1	u	u^2	u^3
u^5	u^5	1	u	u^2	u^3	u^4

Existuje cyklická grupa *I* řádu šest a grupy s ní izomorfní. Z její operační tabulky opět můžeme vyčíst její vlastnosti. A tato tabulka ukazuje její konstrukci.

Je-li *G* necyklická grupa řádu šest, potom podle důsledku Lagrangeovy věty mají její nejednotkové prvky řád dva nebo tři. Nejprve si ukážeme, že v *G* musí existovat prvek řádu tři. V opačném případě by v *G* existovaly pouze nejednotkové prvky řádu dva, například $u \neq v$. Potom vy ale *G* musela nutně obsahovat Kleinovu čtyřgrupu H, což ale podle Lagrangeovy věty není možné. V *G* tedy musí existovat prvek $u \neq 1$ takový, že platí $u^3 = 1$. Kromě prvků $1, u, u^2 = v$ musí ještě *G* obsahovat další prvek *w* a snadno nahlédneme, že také $w^2 = 1$. Připomeňme si, že v grupě platí zákon krácení zleva i zprava, proto tedy možnosti $w^2 = w, w^2 = uw$ i $w^2 = u^2 w$ vedou ke sporu s tím, že $w \neq 1$, *u* i u^2. Kdyby totiž neplatilo $w^2 = 1$, potom by řád prvku *w* byl tři, a tedy $w^3 = 1$. Ale $w^2 = u$ vede ke sporu, protože $w^3 = uw = 1 = x$ a také možnost $w^2 = u^2$ vede ke sporu $1 = w^3 = u^2 w = y$. Platí tedy $w^2 = 1$. Podobně lze dokázat rovnosti $x^2 = y^2 = 1$. Určíme si ještě, čemu je roven prvek *wu*. Možnosti $wu = 1 = w^2$, $wu = u$, $wu = u^2$ i $wu = w$ vedou ihned ke sporu. Kdyby $uw = wu$, potom po vynásobení prvkem $u^2 w$ zleva dostaneme $u^2 wuw = 1 = yx \Rightarrow x^2 = xy \Rightarrow x = y$, což je spor. Musí tedy platit $wu = u^2 w = y$.

Nyní můžeme napsat operační tabulku této grupy (po provedení několika pomocných výpočtů).

G	**1**	**u**	**v**	**w**	**x**	**y**
1	1	u	v	w	x	y
u	u	v	1	x	y	w
v	v	1	u	y	w	x
w	w	y	x	1	v	u
x	x	w	y	u	1	v
y	y	x	w	v	u	1

Z operační tabulky je vidět, že jde o nekomutativní algebraickou strukturu. Zbývá pouze ověřit, zda jde o grupu. Toto ověření lze provést bezprostředně na základě operační tabulky, ale například ověření asociativnosti je (vzhledem k řádu grupy) poměrně náročné. Vidíme ale, že zobrazení φ definované: $\varphi(1) = Id$, $\varphi(\mathrm{u}) = (123)$, $\varphi(\mathrm{v}) = (132)$, $\varphi(\mathrm{w}) = (12)$, $\varphi(\mathrm{x}) = (23)$, $\varphi(\mathrm{y}) = (13)$ je izomorfismem G na S_3, kde S_3 je symetrická grupa stupně tři.

Definice 11

Symetrickou grupou stupně n rozumíme množinu všech permutací množiny $M = \{1, 2, 3, \ldots, n\}$ společně s operací skládání permutací definovanou jako:

$\pi_1\pi_2(i) = \pi_2(\pi_1(i))$, kde $i = 1, 2, 3, \ldots, n$.

Využíváme známého poznatku, že skládání zobrazení a speciálně permutací je asociativní. Díky tomu není nutné ověřovat asociativnost pro všechny trojice prvků, což by dalo značnou práci. Tím získáváme tento závěr:

Každá grupa řádu šest je tedy izomorfní buďto s cyklickou grupou řádu šest, anbo se symetrickou grupou řádu šest.

Některé grupové konstrukce

Je zřejmé, že s rostoucím řádem vzrůstají i potíže s konstrukcí grup. V následující definici je uveden způsob, jak lze „z menších grup vytvářet větší“.

Definice 12

Mějme grupy *A, B*. Množina *G* všech uspořádaných dvojic (a,b), $a \in A$, $b \in B$, spolu s binární operací $(a_1, \mathrm{b}_1)\cdot(a_2, \mathrm{b}_2) = (a_1 a_2, \mathrm{b}_1 b_2)$ je opět grupou, kterou nazveme vnější direktní součin grup *A, B* a značíme ji $A \times B = G$.

POZNÁMKA: Tento pojem můžeme snadno zobecnit na konečný počet grup $A_1, A_2, A_3, \ldots, A_n$.

K pojmu direktního součinu lze dojít ještě i jiným způsobem. Připomeňme se, že spojením $A \vee B$ dvou podgrup *A* a *B* grupy *G* rozumíme nejmenší podgrupu grupy *G* obsahující *A* i *B*, to znamená $A \vee B = \{A \cap B\}_G$. Je-li buď $A \Delta G$, anebo $B \Delta G$, potom $A \vee B = AB = BA$, $BA = \{ab, a \in A, b \in B\}$.

Definice 13

Mějme dvě normální podgrupy *A, B* grupy *G*. Pokud $A \vee B = G$ a $A \cap B = 1$, řekneme, že *G* je vnitřním direktním součinem grup *A, B*, a značíme ho $A \times B = G$.

Lemma 3

Grupa *G* je direktním součinem svých podgrup *A, B* právě tehdy, když platí: $((\forall \mathrm{a} \in \mathrm{A}, \mathrm{b} \in \mathrm{B}) : \mathrm{ab} = \mathrm{ba})$ a libovolný prvek $g \in G$ lze napsat jednoznačně až na pořadí ve tvaru $g = ab$, $a \in A, b \in B$.

Není potřeba rozlišovat mezi vnitřním a vnějším direktním součinem, což dokážeme velice snadno: Mějme dvě grupy *A, B* a $G = A \times B$ je jejich direktní součin. Označíme-li $A' = \{(a,1), a \in A\}$, je zobrazení $\varphi(\mathrm{a}) = (\mathrm{a},1)$ izomorfismem *A* na A', podobně i $B \cong B'$. Rovnost $(a,1)(1,\mathrm{b}) = (\mathrm{a},\mathrm{b}) = (1,\mathrm{b})(\mathrm{a},1)$ ukazuje, že *G* je vnitřním direktním součinem svých podgrup *A, B* a je-li G' vnějším direktním součinem svých podgrup *A, B*, a je-li G'

vnějším direktním součinem svých grup *A, B,* potom $G' \cong G$ (zobrazení $\varphi(a,b) = ab$, přitom $A' \cong A$ a $B' \cong B$).

Věta 9

Direktní součin dvou grup nesoudělných řádů *m, n* je cyklickou grupou řádu *mn.*

Důkaz

Buď $A = \{a\}$ cyklická grupa řádu *m* a $B = \{b\}$ cyklická grupa řádu *n*. Potom $G = A \times B$ obsahuje prvky tvaru $a^x b^y$, $0 \le r < m$, $0 \le s < n$, a tedy $o(G) \le mn$. Nyní ukažme, že prvek *ab* má v *G* řád *mn.* Je tedy $(ab)^{mn} = a^{mn} \cdot b^{mn} = 1$. Kdyby pro jisté *t* bylo $(ab)^t = 1$, potom by bylo $1 = (ab)^{mt} = a^{mt} \cdot b^{mt}$, takže *n/mt* a vzhledem k $(n,m) = 1$ *n/t.* Analogicky se ukáže, že *m/t,* a tedy $[m,n]/t$. Čísla *m, n* jsou však nesoudělná, a proto $[m,n] = mn$. Řád prvku *ab* v *G* je proto tedy *mn* a $G = \{ab\}$.

Konečné komutativní grupy

Definice 14

Abelova grupa *G*, která nemá prvky nekonečného řádu, se nazývá periodická (neboli torzní) grupa.

Věta10

Nechť *G* je libovolná Abelova grupa. Potom množina $G_p = \{g \in G, o(g) = p^n, n \in N_0\}$, kde *p* je prvočíslo, je podgrupou grupy *G*.

Důkaz

Mějme $a, b \in G$, dále nechť $o(a) = p^r$, $o(\mathrm{b}) = p^s$, $r \geq s$. Potom i $g^{-1} \in G_p$, protože $o(g^{-1}) = \mathrm{p}^r$ a $ab \in G_p$, protože $(ab)^{pr} = a^{pr} \cdot b^{pr} = 1$, proto tedy $o(ab) \leq p^r$.

Definice 16

Konečná grupa řádu p^n, $n \in N$, kde p je prvočíslo, je nazývána p-grupou.

Věta 11

Každá grupa, která je periodická, je direktním součinem svých p-primárních komponent.

Věta 12

Nechť *G* je Abelova grupa a *x* je její prvek maximálního řádu p^k. Potom je cyklická grupa $\{x\}$ direktním součinem v *G*, to znamená že $G = \{x\} \times A$. (Fakt, že *x* je prvek maximálního řádu v *G* znamená, že pro všechna $g \in G$ platí, že $o(g) \leq p^k$.)

Věta 13

Každá konečná Abelova p-grupa je direktním součinem grup cyklických.

Důkaz

Mějme cyklickou grupu *G* řádu *p*. Buď *G* grupa řádu p^n, $n>1$, a předpokládejme, že každá Abelova p-grupa řádu menšího než p^n již je direktním součinem cyklických grup. Je-li $x \in G$ prvek maximálního řádu v *G*, potom je $G = \{x\} \times A$. Ovšem ale *A* je podle indukčního předpokladu direktním součinem cyklických grup, což tedy znamená, že je důkaz dokončen.

Věta 14

Je-li *G* konečná Abelova p-grupa a je-li *G* direktním součinem cyklických grup $G = Z_p^{m_1} \times Z_p^{m_2} \times Z_p^{m_3} \times \ldots \times Z_p^{m_n}$, potom jsou čísla $m_1, m_2, m_3, \ldots, m_n$ určena grupou *G* jednoznačně.

Nechť *G* je konečná Abelova grupa. Užitím vět 11 a 13 zajistíme existenci direktního rozkladu, přičemž řády cyklických direktních činitelů jsou určeny grupou jednoznačně (podle věty 14). Tyto řády cyklických direktních činitelů nazveme invarianty grupy *G*. Dvě konečné Abelovy grupy jsou izomorfní právě tehdy, když mají stejné soustavy invariantů. Ke každé soustavě invariantů existuje určitá konečná komutativní grupa, jejíž soustava invariantů se rovná předem dané soustavě invariantů.

Postup pro nalezení všech komutativních grup řádu *n*:

a) Je-li $n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$ zápis čísla *n* v kanonickém tvaru, je *G* podle věty 11 direktním součinem svých p_i-primárních komponent G_{pi}, $i = 1, 2, 3, \ldots, \mathrm{r}$. Potom řád komponenty G_{pi} je jistě $p_i^{m_i}$, kde $i = 1, 2, 3, \ldots, \mathrm{r}$.

b) Dle věty 13 je každá grupa G_{pi} direktním součinem cyklických grup řádů $p_i^{m_{i_1}}, p_i^{m_{i_2}}, p_i^{m_{i_3}}, \ldots, p_i^{m_{i_s}}$, kde $m_{i_1} + m_{i_2} + m_{i_3} + \ldots + m_{i_{si}} = m_i$, kde $i = 1, 2, 3, \ldots, \mathrm{r}$, $s_i \in N$. Pro nalezení všech možných direktních rozkladů komponenty G_{pi} je tedy nutné nalézt všechna vyjádření čísla m_i ve tvaru součtu několika sčítanců z *N*. (Připouštíme i „součet“ o jednom sčítanci $m_{i_1} = m_i$.)

c) K eventuálnímu zjednodušení direktního rozkladu grupy *G* využijeme větu 11. Teď již můžeme snadno popsat komutativní grupy neprvočíselných řádů *n*.

Příklad 4

$n = 4$:

možné součty jsou 2, 1+1

možné invarianty: a) $2^1, 2^1 \ldots\ldots G_1 = Z_2 \times Z_2$

b) $2^2 \ldots\ldots G_2 = Z_4$

Dostaneme grupy, který už jsme sestrojili v předchozím textu. V případě a) jde o Kleinovu čtyřgrupu, v případě b) jde o cyklickou grupu řádu čtyři.

Příklad 5

$n = 6$:

možné invarianty: a) $2^1, 3^1, \ldots\ldots G_6 = Z_2 \times Z_3 \cong Z_6$ dle věty 9.

Existuje pouze jediná komutativní grupa řádu šest, a to cyklická grupy.

Příklad 6

$n = 8$:

možné součty: $2^3, 3 = 2+1 = 1+1+1$

možné invarianty: a) 2^3

b) $2^2, 2^1$

c) $2^1, 2^1, 2^1$

a) Dostaneme cyklickou grupu řádu 8.

b) Těmito invarianty je určena grupa $G = Z_4 \times Z_2$. Nechť je první cyklická grupa generovaná prvkem u, $u^4 = 1$, druhá prvkem v, $v^2 = 1, uv = vu$.

G	**1**	**u**	**u²**	**u³**	**v**	**uv**	**u²v**	**u³v**
1	1	u	u^2	u^3	v	uv	u^2v	u^3v
u	u	u^2	u^3	1	uv	u^2v	u^3v	v
u³	u^3	1	u	u^2	u^3v	v	uv	u^2v
v	v	uv	u^2v	u^3v	1	u	u^2	u^3
uv	uv	u^2v	u^3v	v	uv	u^2	u^3	1
u²v	u^2v	u^3v	v	uv	u^2	u^3	1	u
u³v	u^3v	v	uv	u^2v	u^3	1	u	u^2

c) Takto je určená grupa $H = Z_2 \times Z_2 \times Z_2$. První grupa je generovaná prvkem *u*, druhá *v* a třetí *w* a platí $u^2 = v^2 = w^2$, $uv = vu$, $uw = wu$, $vw = wv$.

H	**1**	**u**	**v**	**w**	**uv**	**uw**	**vw**	**uvw**
1	1	u	v	w	uv	uw	vw	uvw
u	u	1	uv	uw	v	w	uvw	vw
v	v	uw	1	vw	u	uvw	w	uw
w	w	uw	vw	1	uvw	u	v	uv
uv	uv	v	u	uvw	1	vw	uw	w
uw	uw	w	uvw	u	vw	1	uv	v
vw	vw	uvw	w	v	uw	uv	1	u
uvw	uvw	vw	uw	uv	w	v	u	1

Příklad 7

$n = 9$:

možné invarianty: a) 3^2

b) $3^1, 3^1$

a) Tímto způsobem je určena cyklická grupa řádu 9.

b) Dostaneme grupu $G = Z_3 \times Z_3$. Nechť je první cyklická grupa generovaná prvkem *u* a druhá prvkem *v*. Nutně musí platit, vzhledem k řádu grupy: $u^3 = v^3 = 1$. Je tedy poměrně jednoduché sestrojit operační tabulku této grupy.

G	**1**	**u**	**u²**	**v**	**v²**	**uv**	**u²v**	**uv²**	**u²v²**
1	1	u	u^2	v	v^2	uv	u^2v	uv^2	u^2v^2
u	u	u^2	1	uv	uv^2	u^2v	v	u^2v^2	v^2
u²	u^2	1	u	u^2v	u^2v^2	v	uv	v^2	uv^2
v	v	uv	u^2v	v^2	1	uv^2	u^2v^2	u	u^2
v²	v^2	uv^2	u^2v^2	1	v	u	u^2	uv	u^2v
uv	uv	u^2v	v	uv^2	u	u^2v^2	v^2	u^2	1
u²v	u^2v	v	uv	u^2v^2	u^2	v^2	uv^2	1	u
uv²	uv^2	u^2v^2	v^2	u	uv	u^2	1	u^2v	v
u²v²	u^2v^2	v^2	uv^2	u^2	u^2v	1	u	v	uv

Příklad 8

$n = 10$:

možné invarianty: a) $2^1, 5^1$

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

Existuje pouze jedna komutativní grupa řádu 10, a to cyklická grupa.

Příklad 9

$n = 12$:

možné invarianty: a) $2^2, 3^1$

b) $2^1, 2^1, 3^1$

a) Tím získáme $G = Z_4 \times Z_3 \cong Z_{12}$, což znamená, že jde o cyklickou grupu řádu 12.

b) Tímto způsobem získáme grupu $H = Z_2 \times Z_2 \times Z_3$. Také platí, že $Z_2 \times Z_3 \cong Z_6$ a tedy $H = Z_2 \times Z_6$. Definující relaci můžeme zapsat takto: $u^2 = v^6 = 1,\ uv = vu$.

H	**1**	**u**	**v**	**v²**	**v³**	**v⁴**	**v⁵**	**uv**	**uv²**	**uv³**	**uv⁴**	**uv⁵**
1	1	u	v	v^2	v^3	v^4	v^5	uv	uv^2	uv^3	uv^4	uv^5
u	u	1	uv	uv^2	uv^3	uv^4	uv^5	v	v^2	v^3	v^4	v^5
v	v	uv	v^2	v^3	v^4	v^5	1	uv^2	uv^3	uv^4	uv^5	u
v²	v^2	uv^2	v^3	v^4	v^5	1	v	uv^3	uv^4	uv^5	u	uv
v³	v^3	uv^3	v^4	v^5	1	v	v^2	uv^4	uv^5	u	uv	uv^2
v⁴	v^4	uv^4	v^5	1	v	v^2	v^3	uv^5	u	uv	uv^2	uv^3
v⁵	v^5	uv^5	1	v	v^2	v^3	v^4	u	uv	uv^2	uv^3	uv^4
uv	uv	v	uv^2	uv^3	uv^4	uv^5	u	v^2	v^3	v^4	v^5	1
uv²	uv^2	v^2	uv^3	uv^4	uv^5	u	uv	v^3	v^4	v^5	1	v
uv³	uv^3	v^3	uv^4	uv^5	u	uv	uv^2	v^4	v^5	1	v	v^2
uv⁴	uv^4	v^4	uv^5	u	uv	uv^2	uv^3	v^5	1	v	v^2	v^3
uv⁵	uv^5	v^5	u	uv	uv^2	uv^3	uv^4	1	v	v^2	v^3	v^4

Příklad 10

$n = 14$:

možné invarianty: a) $2^1, 7^1$

Tímto způsobem získáme grupu $H = Z_2 \times Z_7 \cong Z_{14}$, což znamená, že jde o cyklickou grupu řádu 14. (Operační tabulku nebudeme sestrojovat, protože by byla velmi obsáhlá.)

Příklad 11

$n = 15$:

možné invarianty: a) $3^1, 5^1$

Tímto způsobem získáme grupu $H = Z_3 \times Z_5 \cong Z_{15}$, a stejně jako v předchozím příkladu se jedná o jedinou grupu, a to cyklickou grupu řádu 15.

Těmito příklady jsme dokázali popsat všechny komutativní grupy řádu *n*, pro $n \leq 15$.

Konečné nekomutativní grupy

V této části se budeme věnovat nekomutativním grupám řádu 8 a 9.

Osmiprvková nekomutativní grupa *G* nesmí obsahovat prvek řádu 8 (protože by se z ní stala grupa komutativní), ale ani nesmí mít nejednotkové prvky řádu 2. Grupa *G* tedy obsahuje prvek řádu 4, označíme ho například *u*. Potom tedy grupa $U = \{u\}$ je cyklickou grupou řádu 4, tedy $[G:U] = 2$.

Je velmi dobře známé, že platí následující tvrzení:

Mějme podgrupu *H* grupy *G* takovou, že $[G:H] = 2$, potom $H \Delta G$.

Proto tedy $U \Delta G$ a faktor-grupa G/U je řádu 2. Nechť $v \in G$ je takový prvek, že $v \notin U$, potom platí, že $(vU)^2 = v^2U = U$, a proto $v^2 \in U$.

Tím jsme ukázali, že $v^2 \in U$. V úvahu připadají následující možnosti $v^2 = u$, $v^2 = u^3$, $v^2 = u^2$, $v^2 = 1$. Pokud by bylo $v^2 = u$, potom by grupa $\{v\}$ byla cyklickou grupou řádu 8, která by obsahovala prvky *v, u, uv, u²*, *u²v*, *u³*, *u³v*, 1, což by byl spor. Pokud by bylo $v^2 = u^3$, potom by zase $\{v\}$ byla cyklickou grupou řádu 8, která by obsahovala prvky *v, u³*, *u³v*, *u²*, *u²v*, *u³*, *u*, *uv*, 1. Zůstaly tedy pouze dvě možnosti, a to $v^2 = u^2$ a $v^2 = 1$.

Přičemž navíc platí $U \Delta G$, proto tedy $v^{-1}uv \in U$. Opět mohou nastat čtyři možnosti, ale $v^{-1}uv = 1$ vede ke sporu $uv = v$, $u = 1$ a vztah $v^{-1}uv = u$ znamená, že $uv = vu$ a G by tím pádem byla komutativní grupou. Nakonec z $v^{-1}uv = u^2$ máme $v^{-1}u^2v = v^{-1}uv$ $v^{-1}uv = u^2$ $u^2 = 1$, to znamená $u^2v = v$, $u^2 = 1$, což vede opět ke sporu. Zbyla tedy pouze jedna jediná možnost, a to $v^{-1}uv = u^3$.

Tím se dá ukázat, že mohou existovat dvě nekomutativní grupy řádu 8, které jsou zadané relacemi:

a) $u^4 = v^2 = 1,\ uv = u^3$

b) $u^4 = 1,\ v^2 = u^2,\ v^{-1}uv = u^3$

a) V tomto případě si převedeme zápisy typu vu^n, $n = 1,2,3$ na tvar $u^r v^s$. Dále je $v^{-1} = v$, $vuv = u^3$, $vu = u^3v$ a $vu^2 = vu \cdot u = u^3vu = u^3 \cdot u^3v = u^2v$, $vu^3 = uv$.

	1	**u**	**u²**	**u³**	**v**	**uv**	**u²v**	**u³v**
1	1	u	u^2	u^3	v	uv	u^2v	u^3v
u	u	u^2	u^3	1	uv	u^2v	u^3v	v
u²	u^2	u^3	1	u	u^2v	u^3v	v	uv
u³	u^3	1	u	u^2	u^3v	v	uv	u^2v
v	v	u^3v	u^2v	uv	1	u^3	u^2	u
uv	uv	v	u^3v	u^2v	u	1	u^3	u^2
u²v	u^2v	uv	v	u^3v	u^2	u	1	u^3
u³v	u^3v	u^2v	uv	v	u^3	u^2	u	1

b) V tomto případě si snadno odvodíme následující rovnosti $vu = u^3v$, $vu^2 = u^2v, vu^3 = uv$. Jako prvky grupy H (pokud tedy existuje) jsou prvky 1, *u*, u^2, u^3, *v*, *uv*, u^2v, u^3v.

H	**1**	**u**	$\mathbf{u^2}$	$\mathbf{u^3}$	**v**	**uv**	$\mathbf{u^2v}$	$\mathbf{u^3v}$
1	1	u	u^2	u^3	v	uv	u^2v	u^3v
u	u	u^2	u^3	1	uv	u^2v	u^3v	v
$\mathbf{u^2}$	u^2	u^3	1	u	u^2v	u^3v	v	uv
$\mathbf{u^3}$	u^3	1	u	u^2	u^3v	v	uv	u^2v
v	v	u^3v	u^2v	uv	u^2	u	1	u^3
uv	uv	v	u^3v	u^2v	u^3	u^2	u	1
$\mathbf{u^2v}$	u^2v	uv	v	u^3v	1	u^3	u^2	u
$\mathbf{u^3v}$	u^3v	u^2v	uv	v	u	1	u^3	u^2

Opět si můžeme ukázat, že jak v případě a), tak i v případě b) jsme získali nekomutativní grupy. Tyto dvě grupy nejsou izomorfní.

Existují dvě neizomorfní nekomutativní grupy řádu 8.

Nyní si popíšeme grupu kvaternionů. Existuje i jiná možnost jak zadat tuto grupu (kromě tabulky), a to taková, že na množině $\{1, -1, a, -a, b, -b, c, -c\}$ rozšíříme násobení komplexních čísel ještě o pravidla: $a^2 = b^2 = c^2 = 1$, $ab = c = -ba$, $bc = a = -cb$, $ca = b = -ac$.

Q_8	**1**	**-1**	**a**	**-a**	**b**	**-b**	**c**	**-c**
1	1	-1	a	-a	b	-b	c	-c
-1	-1	1	-a	a	-b	b	-c	c
a	a	-a	-1	1	c	-c	-b	b
-a	-a	a	1	-1	-c	c	b	-b
b	b	-b	-c	c	-1	1	a	-a
-b	-b	b	c	-c	1	-1	-a	a
c	c	-c	b	-b	-a	a	-1	1
-c	-c	c	-b	b	a	-a	1	-1

Z tabulky je patrné, že tabulka grupy *G* a tabulka grupy kvaternionů Q_8, že obě tyto grupy jsou izomorfní. Grupa kvaternionů je zajímavá i tím, že se sice jedná o nekomutativní grupu, ale každá její podgrupa je normální podgrupou grupy Q_8.

Definice 16

Mějme grupu *G*. Množina $S = \{s \in G, sg = gs \forall g \in S\}$ se nazývá centrum grupy *G*.

Věta 15

Nechť je centrum z libovolné grupy *G* komutativní podgrupou grupy *G*. Potom každá podgrupa centra grupy *G* je normální podgrupou grupy *G*.

Věta 16

Každá konečná p-grupa má netriviální centrum, to znamená, že prvočíslo *p* dělí řád centra *S*.

Grupa řádu 9 je tzv. 3-grupa. Centrum této grupy je podgrupa, a to s ohledem na větu 16 buďto tříprvková, anebo devítiprvková. V druhém případě je však $S = G$, a *G* je komutativní. Nekomutativní grupa *G* by musela nutně mít tříprvkové centrum, $S = \{v\}$, $v^3 = 1$. Poté také musí existovat $u \in G$, ale zároveň $u \notin S$. Ovšem také $u^2 \notin S$ a prvek *u* je

řádu 3 v *G*. Dále také platí $\{u\} \cap \{v\} = 1$, $v \in S$, z čehož plyne $uv = vu$. Z toho také plyne možnost uvést všechny součiny prvků *u, v* do tvaru $u^x v^y$, kde $0 \le x \le 2$ a $0 \le y \le 2$, takže devítiprvková grupa *G* obsahuje pouze prvky tohoto tvaru. Ovšem prvek *u* komutuje s každým prvkem ve tvaru $u^x v^y$, z čehož plyne, že $u \in S$, přičemž dochází ke sporu. Na závěr můžeme konstatovat, že neexistuje žádná nekomutativní grupa řádu 9.

Další část věnujeme studiu nekomutativních grup řádu *pq*, kde *p, q* jsou navzájem různá prvočísla.

Definice 17

Mějme grupu *G* řádu $p^a b$, kde $(p,b) = 1$. Potom každá podgrupa grupy *G* řádů p^a se nazývá Sylowovská p-grupa grupy *G*.

Definice 18

Nechť *G* je grupa, $g, h \in G$. Prvek *h* je konjugován prvkem *g* právě tehdy, když existuje takový prvek $k \in G$, že $h = k^{-1} g k$. Podobně podgrupy *H, I* grupy *G* jsou konjugovány v *G* právě tehdy, když existuje prvek $k \in G$ takový, že $I = k^{-1} H k$.

Věta 17

Nechť *G* je konečnou grupou řádu *a* a *p* je prvočíslo, které dělí *a*. Potom *G* obsahuje sylowovskou p-podgrupu.

Pro sestavování operačních tabulek grup řádu *pq* je za potřebí využít Sylowovy věty:

První Sylowova věta

Každá p-podgrupa *A* konečné grupy *B* je obsažena v některé sylowovské p-podgrupě grupy *B*.

Druhá Sylowova věta

Každé dvě sylowovské p-podgrupy konečné grupy *B* jsou konjugované.

Třetí Sylowova věta

Mějme konečnou grupu *B* a *p* je prvočíslo, které dělí řádgrupy *B*. Potom počet všech sylowovských p-podgrup grupy *B* dělí $o(B)$ a je roven $1+zp$, kde *z* je nějaké určité záporné číslo.

Připomeňme si, že v případě, kdy grupa *B* obsahuje sylowovskou p-podgrupu *P*, musí být podle druhé Sylowovy věty konjugována sama se sebou. Pro každé $b \in B$ je potom $b^{-1}Pb = P$ a sylowovská p-podgrupa *P* je v tomto případě normální podgrupou grupy *B*.

Nyní si popíšeme grupu řádu 10. Desetiprvková grupa *B* obsahuje sylowovské 5-podgrupy, kterých je podle třetí Sylowovy věty $1+5n$, $n = 0,1,2,\ldots$ a zároveň $1+5n$ dělí 10. V tomto případě vyhovuje pouze $n = 0$, což znamená, že v *B* existuje jediná sylowovská 5-podgrupa *U*. Navíc *U* je normální podgrupou grupy *B* a zároveň pětiprvkovou cyklickou grupou s generátorem *u*. Proto tedy $U = \{u\}, u^5 = 1$ a $U \Delta B$.

Grupa *U* zároveň obsahuje sylowovské 2-podgrupy. Těchto podgrup je $1+2m$, $m = 0,1,\ldots$ a zároveň $1+2m$ dělí 10. V tomto případě vyhovuje $m = 0$ a $m = 2$.

a) $m = 0$

Grupa *B* má jedinou sylowovskou 2-podgrupu $\{v\}$, $v^2 = 1$, $v \Delta B$. Podgrupy $\{u\}$ a $\{v\}$ jsou normální podgrupy grupy *B* nesoudělných řádů, obě jsou cyklické, což znamená, že $B = \{u\} \times \{v\}$ je cyklická grupa řádu 10.

b) $m = 2$

Grupa *B* má pět sylowovských 2-podgrup. Jednu z nich označíme $\{v\}, v^2 = 1$. $U \Delta B$, proto $v^{-1}uv \in U$, to znamená, že $v^{-1}uv = u^k$, kde $k = 1,2,3,4,5$. Dále také platí, že $u = v^{-2}uv^2 = v^{-1}v^{-1}uvv = v^{-1}u^k v = v^{-1}uv \cdot v^{-1}$, $uv \cdot \ldots \cdot v^{-1}$ (tento činitel se k-krát opakuje) == u^{k^2}, a protože prvek *u* je řádu 5, dává u^2 při dělení číslem 5 zbytek 1. Této podmínce vyhovují $k = 1$ nebo $k = 4$. Pokud by $v^{-1}uv = u$, potom by bylo $uv = vu$ a dostali bychom komutativní grupu. Zbývá nám tedy jen možnost $k = 4$.

Mějme tedy tyto definující relace: $u^5=1,\ v^2=1,\ v^{-1}uv=u^4$. Převedeme si ještě zápisy typu vu^k, $k=1,2,3,4$, do tvaru u^rv^s. Vynásobíme poslední z definujících relací prvkem *v* zleva a dostaneme $vu^4=uv$.

Dále potom:

$$vu^3=vu^3\cdot u^5=vu^4\cdot u^4=uvu^4=u^2v$$

$$vu^2=vu^2\cdot u^5=vu^4\cdot u^3=uvu^3=u^3v$$

$$vu=vu\cdot u^5=vu^4\cdot u^2=uvu^2=u^4v$$

Opět lze ověřit, že uvedenými definujícími relacemi $u^5=1,\ v^2=1,\ v^{-1}uv=u^4$ je opravdu daná grupa.

	1	**u**	**u²**	**u³**	**u⁴**	**v**	**uv**	**u²v**	**u³v**	**u⁴v**
1	1	u	u²	u³	u⁴	v	uv	u²v	u³v	u⁴v
u	u	u²	u³	u⁴	1	uv	u²v	u³v	u⁴v	v
u²	u²	u³	u⁴	1	u	u²v	u³v	u⁴v	v	uv
u³	u³	u⁴	1	u	u²	u³v	u⁴v	v	uv	u²v
u⁴	u⁴	1	u	u²	u³	u⁴v	v	uv	u²v	u³v
v	v	uv	u²v	u³v	u⁴v	1	u⁴	u³	u²	u
uv	uv	v	u⁴v	u³v	u²v	u	1	u⁴	u³	u²
u²v	u²v	uv	v	u⁴v	u³v	u²	u	1	u⁴	u³
u³v	u³v	u²v	uv	v	u⁴v	u³	u²	u	1	u⁴
u⁴v	u⁴v	u³v	u²v	uv	v	u⁴	u³	u²	u	1

Existují dvě neizomorfní grupy řádu 10, jedna je nekomutativní a druhá je cyklická.

Nyní si popíšeme grupu řádu 14. Grupy, které mají 14 prvků, obsahují sylowovské 7-podgrupy, kterých je $1+7m$, a zároveň $1+7m$ dělí 14. V tomto případě vyhovuje pouze $m=0$. Existuje tedy jedna jediná sylowovská 7-podgrupa, která je normální podgrupou

grupy *B*. Označíme ji $\{u\}$, $u^7 = 1$. Grupa *B* má dále také $1+2r$ sylowovských 2-podgrup. V úvahu přicházejí tyto možnosti: $r = 0$, anebo $r = 3$.

a) $r = 0$

V tomto případě existuje jedna jediná sylowovská 2-podgrupa $\{v\}$, $v^2 = 1$, která je normální podgrupou grupy *B*. Je tedy patrné, že $B = \{u\} \times \{v\}$, což znamená, že *B* je cyklická grupa.

b) $r = 3$

V tomto případě existuje 7 sylowovských 2-podgrup. Jedna z nich je $\{v\}$, $v^2 = 1$. Podgrupa $\{v\}$ sice není normální podgrupou grupy *B*, ale $\{u\}$ už ano, z toho vyplývá, že $v^{-1}uv = u^k$, kde *k* je určité přirozené číslo, *k* < 8. Stejně jako v případě grupy řádu 10 můžeme odvodit $u^1 = u^{k^2}$, což znamená, že $k^2 \equiv 1 \bmod 7$. Tím dostaneme, že $k = 1$ nebo $k = 6$. První z možností vede ke komutativní grupě *B*. Její definující relace jsou: $u^7 = 1$, $v^2 = 1$, $v^{-1}uv = u^6$. Převedením zápisu z tvaru vu^x do tvaru $u^n v$ získáme tyto relace: $vu^6 = uv$, $vu^5 = u^2v$, $vu^4 = u^3v$, $vu^3 = u^4v$, $vu^2 = u^5v$ $vu = u^6v$.

	1	**u**	**u^2**	**u^3**	**u^4**	**u^5**	**u^6**	**v**	**uv**	**u^2v**	**u^3v**	**u^4v**	**u^5v**	**u^6v**
1	1	u	u^2	u^3	u^4	u^5	u^6	v	uv	u^2v	u^3v	u^4v	u^5v	u^6v
u	u	u^2	u^3	u^4	u^5	u^6	1	uv	u^2v	u^3v	u^4v	u^5v	u^6v	v
u^2	u^2	u^3	u^4	u^5	u^6	1	u	u^2v	u^3v	u^4v	u^5v	u^6v	v	uv
u^3	u^3	u^4	u^5	u^6	1	u	u^2	u^3v	u^4v	u^5v	u^6v	v	uv	u^2v
u^4	u^4	u^5	u^6	1	u	u^2	u^3	u^4v	u^5v	u^6v	v	uv	u^2v	u^3v
u^5	u^5	u^6	1	u	u^2	u^3	u^4	u^5v	u^6v	v	uv	u^2v	u^3v	u^4v
u^6	u^6	1	u	u^2	u^3	u^4	u^5	u^6v	v	uv	u^2v	u^3v	u^4v	u^5v
v	v	u^6v	u^5v	u^4v	u^3v	u^2v	uv	1	u^6	u^5	u^4	u^3	u^2	u
uv	uv	v	u^6v	u^5v	u^4v	u^3v	u^2v	u	1	u^6	u^5	u^4	u^3	u^2
u^2v	u^2v	uv	v	u^6v	u^5v	u^4v	u^3v	u^2	u	1	u^6	u^5	u^4	u^3
u^3v	u^3v	u^2v	uv	v	u^6v	u^5v	u^4v	u^3	u^2	u	1	u^6	u^5	u^4
u^4v	u^4v	u^3v	u^2v	uv	v	u^6v	u^5v	u^4	u^3	u^2	u	1	u^6	u^5
u^5v	u^5v	u^4v	u^3v	u^2v	uv	v	u^6v	u^5	u^4	u^3	u^2	u	1	u^6
u^6v	u^6v	u^5v	u^4v	u^3v	u^2v	uv	v	u^6	u^5	u^4	u^3	u^2	u	1

Existují dvě neizomorfní grupy řádu 14, přičemž jedna z nich je cyklická grupa a grupa G, která je určení relacemi $u^7 = 1,\ v^2 = 1$ a $v^{-1}uv = u^6$.

Na závěr si probereme grupu řádu 15. Grupa řádu 15 obsahuje sylowovskou 5-podgrupu, a to pouze jedinou, která je normální podgrupou grupy *B*. To samé platí pro sylowovské 3-podgrupy. Protože $(3,5) = 1$, existuje až na izomorfismus pouze jedna jediná grupa řádu 15, kterou můžeme dostat jako direktní součin cyklických grup řádu 3 a řádu 5. Můžeme tedy konstatovat, že neexistuje žádná nekomutativní grupa řádu 15.

Poznamenejme ještě, že v obecném případě pro grupy řádu *pq*, kdy $p < q$ jsou prvočísla, platí tvrzení:

a) Vždy existuje cyklická grupa řádu *pq*.

b) V případě, pokud p dělí q-1, existuje také nekomutativní grupa, která je definována operacemi $u^p = 1,\ v^q = 1,\ v^{-1}uv = u^k$, přičemž číslo $k \neq 1$ je nějakým řešením kongruence $k^q \equiv 1 \bmod q$.

V této části jsme se věnovali komutativním a nekomutativním grupám řádů $n \leq 15$. Závěry můžeme shrnout do následující tabulky:

n	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Počet grup řádu n	1	1	2	1	2	1	5	1	2	1	5	1	2	1
Komutativní grupy	1	1	2	1	1	1	3	1	1	1	2	1	1	1
Nekomutativní grupy	0	0	0	0	1	0	2	0	1	0	3	0	1	0

Základní pojmy teorie okruhů malých řádů

Definice 19

Nechť okruh $R(\oplus,\otimes)$ je neprázdná množina se dvěma operacemi, pro které platí:

a) $R(\oplus)$ je Abelova grupa

b) $(\forall x, y, z \in R): x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$

c) $(\forall x, y, z \in R): (x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z)$.

POZNÁMKA: Pokud je $R(\oplus,\otimes)$ okruh, potom Abelova grupa $R(\oplus)$ aditivní grupou okruhu R a $R(\otimes)$ je multiplikativní grupou okruhu R.

Definice 20

Mějme okruh $R(\oplus,\otimes)$, který nazveme triviálním okruhem právě tehdy, když má jen jeden prvek. V opačném případě se tento okruh nazývá netriviální.

Definice 21

Mějme okruh $R(\oplus,\otimes)$, který nazveme asociativním okruhem, pokud tuto vlastnost má jeho multiplikativní grupou, tedy pokud platí:
$(\forall x, y, z \in R): x \otimes (y \otimes z) = (x \otimes y) \otimes z$.

Definice 22

Mějme okruh $R(\oplus,\otimes)$, který nazveme komutativním okruhem, jestliže má tuto vlastnost jeho multiplikativní grupou, tedy pokud platí: $(\forall x, y, \in R): x \otimes y = y \otimes x$.

Definice 23

Pokud je R asociativní okruh, potom multiplikativní grupou je pologrupa a mluvíme o multiplikativní pologrupě okruhu $R(\oplus,\otimes)$.

Definice 24

Prvek $a \in R$ nazveme levým (popřípadě pravým) jednotkovým prvkem okruhu $R(\oplus, \otimes)$, pokud $a \otimes x = x$ (popřípadě $x \otimes a = x$).

Definice 25

Mějme okruh $R(\oplus, \otimes)$. Dále prvek $b \in R$ nazveme zleva (popřípadě zprava) dělící, pokud zleva (popřípadě zprava) dělí každý prvek multiplikativního grupoidu $R(\otimes)$. Pokud je každý nenulový prvek okruhu $R(\oplus, \otimes)$ zleva (popřípadě zprava) dělící, potom $R(\oplus, \otimes)$ nazveme okruhem s levým (popřípadě pravým) dělením.

POZNÁMKA: Nulový prvek je dělící právě tehdy, když $R(\oplus, \otimes)$ je triviálním okruhem.

Definice 26

Číslo $k \in N$ nazveme charakteristikou okruhu $R(\oplus, \otimes)$, pokud $k \times m = 0$ pro každé $m \in R$ a pokud *k* je nejmenším číslem v *N* s touto vlastností. Pokud v *N* neexistuje takové číslo, potom charakteristikou okruhu rozumíme $0 \in N_0$ (v obou případech použijeme značení $char(R)$ a také platí, že $char(R) \in R$.

Definice 27

Mějme okruh $R(\oplus, \otimes)$. Neprázdnou podmnožinu *A* množiny *R* nazveme podokruhem okruhu $R(\oplus, \otimes)$ právě tehdy, když *A* je současně podgrupa aditivní grupy a podgrupou multiplikativního okruhu *R*. Používáme značení $A \leq R$.

Definice 28

Mějme okruhy $R(\oplus, \otimes)$ a $A(+, \times)$. Zobrazení $\varphi : R \to A$ nazveme homomorfismem okruhů, pokud je φ zároveň homomorfismus aditivních grup a multiplikativních grupoidů. Což znamená, že $\forall x, y \in R$
$\varphi(x \oplus y) = \varphi(x) \oplus \varphi(y) \wedge \varphi(\mathrm{x} \otimes \mathrm{y}) = \varphi(\mathrm{x}) \otimes \varphi(\mathrm{y})$.

Bijektivní homomorfismus okruhů nazveme izomorfismem okruhů.

Okruhy s cyklickou aditivní grupou

Aditivní grupy okruhů jsou abelovské, a jelikož jsou řádu menšího než 8, jsou všechny cyklické, tedy až na jednu grupu z řádu 4 (jde o tzv. Kleinovu čtyřgrupu V). Proto má smysl tento cyklický případ diskutovat zvlášť.

Nejprve uveďme, že každý okruh, jehož aditivní grupa je cyklická, je nutně komutativní. Pokud má aditivní grupa okruhu generátor *u*, pak každý prvek může být vyjádřen ve tvaru $u+u+u+\ldots+u=nu$, kde *n* je celé číslo, a potom pokud je například prvek $v=n_1u$ a prvek $w=n_2u$, pak $v\cdot w=(n_1u)\cdot(n_2u)=(n_1n_2)u^2=(n_2u)\cdot(n_1u)=w\cdot v$. Všechny okruhy, které si určíme, budou komutativní, s výjimkou těch, které mají aditivní grupu V.

Určování všech diskutovaných okruhů bude jeden problém. Dalším úkolem je však popsat všechny vzájemně izomorfní okruhy. Mějme okruh *X* řádu *n*, který má cyklickou aditivní grupu C_n a generátor *x*. Dále nechť $x^2=kx$, kde $0\le k\le n-1$. Celá čísla *n* a *k* určují okruh jednoznačně, protože $(k_1x)(k_2x)=(k_1k_2)x^2=(k_1k_2k)x$. Obdobně mějme okruh *Y* s aditivní grupou C_n a generátorem *y*, a nechť $y^2=l\cdot y$, kde $0\le l\le n-1$.

Dále také předpokládejme, že $\varphi: X\to Y$ je izomorfismus, kde platí $\varphi(x)=m\cdot y$. Protože φ je zobrazení *X* na *Y*, tak musí existovat $k_1x\in X$ takové, že $\varphi(k_1x)=y$; což znamená, že $y=\varphi(k_1x)=k_1\varphi(x)=k_1m\cdot y$. Z toho plyne, že musí platit $k_1m\equiv 1 \bmod n$, takže k_1m-1 musí být násobkem čísla *n*. Speciálně, největší společný dělitel (*m, n*) je roven jedné. Vzhledem k tomu, že φ je okruhovým homomorfismem, $kmy=\varphi(kx)=\varphi(x^2)=\varphi(x)\cdot\varphi(x)=m^2y^2=m^2ly$, proto $km\equiv m^2l \bmod n$. Protože (*m, n*) = 1, můžeme vydělit *m* a máme $k\equiv ml \bmod n$. Na konec (*k, n*) dělí *k* i *n*, proto dělí i *ml*; ale (*m, n*) = 1 a proto (*k, n*) dělí *l*. Naopak každý dělitel čísel *l* i *n*, musí nutně dělit *k*. Z toho plyne, že $(k,n)=(l,n)$.

Věta 18

Buď *X* a *Y* dva izomorfní okruhy s aditivní grupou C_n generovanou prvky *x*, respektive *y*, kde $x^2 = k \cdot x$ a $y^2 = l \cdot y$. Potom platí $(k,n) = (l,n)$.

Obrácená věta platí také. Jsou-li tedy *X* a *Y* dva okruhy, které mají aditivní grupu C_n a generátory *x*, respektive *y*, kde $x^2 = k \cdot x$ a $y^2 = l \cdot y$, a pokud $(k,n) = (l,n)$, potom jsou *X* a *Y* izomorfní okruhy.

Sloučením těchto tvrzení získáme nutnou a postačující podmínku pro to, aby okruhy se stejnou aditivní grupou byly izomorfní. Jako důsledek dostaneme počet navzájem různých okruhů.

POZNÁMKA: Existuje tolik různých (neizomorfních) okruhů, které mají aditivní grupu C_n, kolik je dělitelů čísla *n*.

Každé kladné číslo *n* má dělitele 1 a *n*. Uvažujme, že platí $x^2 = 1 \cdot x = x$. Pak $(k_1 x)(k_2 x) = (k_1 k_2)x^2 = (k_1 k_2)x = (\bar{k}_1 \cdot \bar{k}_2)x$, kde $(\bar{k}_1 \cdot \bar{k}_2)$ představuje zbytek při dělení čísla $k_1 k_2$ číslem *n*. Z toho vyplývá, že okruh je izomorfní okruhu Z_n při zobrazení $k \cdot x \to k$.

Dále předpokládejme, že $x^2 = 1 \cdot x = 0$. Potom platí $(k_1 x)(k_2 x) = (k_1 k_2)x^2 = 0$, čímž získáváme triviální okruh O_n, ve které je součin dvou libovolných prvků vždy roven nule.

Poznamenejme, že Z_n je komutativní okruh s jednotkou (pro $n \geq 2$), zatímco O_n nejspíš jednotku nemá. Jestli je $n = 1$, potom okruh obsahuje pouze samotný nulový prvek a Z_n a O_n splývají. Pokud je *n* prvočíslo, jsou 1 a *n* jedinými děliteli čísla *n* a proto Z_n a O_n jsou jediné možné okruhy s aditivní grupou C_n. Tím jsme vyřešili případy, kdy $n = 2,3,5,7$.

Pokud je $n = 4$, potom existují tři dělitelé a tři okruhy. Třetí okruh je dán relací $x^2 = 2x$ (uveďme, že největší společný dělitel $(1,4) = (3,4)$, proto tedy $x^2 = 3x$, což dává znovu Z_4) a je komutativní, netriviální a nemá jednotkový prvek.

Pokud $n = 6$, potom existují čtyři okruhy. Dva z nich odpovídají okruhům dříve popsaným, třetí a čtvrtý jsou určeny relacemi $x^2 = 2x$ a $x^2 = 3x$. Okruh, který je definovaný relací $x^2 = 2x$ ztotožníme s $Z_3 \oplus O_2$. Pokud vezmeme množinu uspořádaných dvojic $[a,b]$, kde $a \in Z_3$ a $b \in O_2$. Jestli označíme *x* jako uspořádanou dvojici $[2,1]$,

potom máme $[2,1]^2 = [2^2, 1^2] = [1,0] = [2,1] + [2,1]$. Obdobně okruh, který je definovaný relací $x^2 = 3x$ nám dá $Z_2 \oplus O_3$, kde $x = [1,1]$.

Je tedy zřejmé, že ze čtyř okruhů Z_6, O_6, $Z_2 \oplus O_3$ a $Z_3 \oplus O_2$ má pouze Z_6 jednotkový prvek. Každé objevení se triviálního okruhu stačí k vyloučení takového prvku. Což platí nejen pro $n = 6$, ale pro jakékoli přirozené *n*.

Věta 19

Až na izomorfismus, jediný okruh *X*, který má jednotkový prvek a aditivní grupu C_n je Z_n.

Důkaz

Buď *x* generátor grupy C_n, kde $x^2 = k \cdot x$, a nechť *jx* je jednotkový prvek. Potom platí $x = (jx)x = jx^2 = jkx$, tedy $jk \equiv 1 \bmod n$. Proto je největší společný dělitel $(k,n) = 1 = (1,n)$ a $X \cong Z_n$.

Dodatek k větě 18 umožňuje nalezení následujících vztahů pro $\psi(n)$ počet okruhů s aditivní grupou C_n. Pokud je *n* mocninou prvočísla *p* (například $n = p^a$), potom $\psi(n) = a + 1$ umožňuje spočítat počet dělitelů čísla *n*. Pokud $n = p_1^{a_1} \cdot p_2^{a_2} \cdot K p_i^{a_i}$ je rozklad čísla *n* na mocniny prvočísel, potom $\psi(n) = \psi(p_1^{a_1}) \cdot \psi(p_2^{a_2}) \cdot \ldots \cdot \psi(p_i^{a_i})$.
Jinak řečeno, ψ je multiplikativní funkce. Opět lze snadno určit počet dělitelů čísla *n*. Spojením obou výsledků v jeden získáme následující tvrzení:

Věta 20

Až na izomorfismus, počet navzájem různých okruhů, které mají cyklickou aditivní grupu C_n, kde $n = p_1^{a_1} \cdot p_2^{a_2} \cdot K p_i^{a_i}$, je dáno výrazem $\psi(n) = (a_1+1)(a_2+1) \cdot \ldots \cdot (a_i+1)$.
Dle věty 19 má pouze jeden z těchto okruhů jednotkový prvek.

Pro ilustraci uvedeme hodnotu $\psi(n)$ pro několik hodnot *n*.

n	1	2	3	4	5	6	7	8	9
$\psi(n)$	1	2	2	3	2	4	2	4	3

n	10	11	12	13	14	15	16	17	18
$\psi(n)$	4	2	6	2	4	4	5	2	6

n	19	20	21	22	p-prvočíslo
$\psi(n)$	2	6	4	8	2

Nekomutativní okruhy

V [1] Erickson dokázal následující výsledek:

Věta 21

Buď *n* přirozené číslo, *n* > 1. Potom existuje nekomutativní okruh řádu *n* právě tehdy, když *n* je dělitelné čtvercem přirozeného čísla. To zajišťuje existenci nekomutativního okruhu řádu 4.

Důkaz

Důkaz rozdělíme na tři části. Nejdříve nahlédneme, že pokud je *n* nedělitelné čtverem, potom okruh řádu *n* je komutativní. Poté zkonstruujeme okruh řádu p^2, kde *p* je prvočíslo. A nakonec zkonstruujeme nekomutativní okruh řádu $k \cdot p^2$, kde *k* je přirozené číslo, *k* >1.

První část důkazu plyne ze základní věty o konečně generovaných Abelových grupách. Uvažujme, že *n* je nedělitelné čtvercem a nechť *X* je aditivní grupa okruhu řádu *n*. Z toho plyne, že *X* může být reprezentována jako direktní součet cyklických grup. Protože je *X* konečná, tak i všechny tyto cyklické grupy jsou konečné. Základní věta nám také umožňuje volit tyto cyklické grupy tak, aby řád každé grupy dělil řád grupy následující, což znamená, že $X = C_{n_1} \oplus C_{n_2} \oplus \ldots C_{n_i}$, kde n_1 >1 a $n_1 \mid n_2 \mid \ldots \mid n_i$.

Teď $n = n_1 \cdot n_2 \cdot \ldots \cdot n_i$, a pokud i >1, potom *n* je dělitelné čtvercem, jestli $n_1 \mid n_2$. Tedy *i* = 1 a $X = C_n$. Jak jsme už viděli, každý okruh, který má aditivní cyklickou grupu musí být komutativní.

Buď *p* prvočíslo, potom utvořme direktní součet grupy C_p opět s C_p. Tím získáme aditivní grupu s p^2 prvky. Abychom mohli zkonstruovat nekomutativní okruh *R* s touto aditivní grupou, musíme si zvolit generátor *a* grupy C_p. Poté uspořádané dvojice $(a,0)$ a $(0,a)$ generují *R* (při aditivním zápisu).

Nadefinujme si násobení těchto uspořádaných dvojic tak, že výsledkem násobení $x \cdot y$ je vždy levý činitel *x*, tedy:

$(a,0)\cdot(a,O) = (a,0)\cdot(0,a) = (a,0)$ a také

$(\mathrm{O},a)\cdot(0,a) = (0,a)\cdot(a,O) = (0,a)$.

Obecně potom násobení v *R* budeme definovat rozšířením právě uvedeného s využitím distributivních zákonů, což znamená:

$$(ka,la)\cdot(ra,sa)=\left\{\overbrace{(a,0)+(a,0)+\ldots+(a,0)}^{k\text{krát}}+\overbrace{(0,a)+(0,a)+\ldots+(0,a)}^{l\text{krát}}\right\}\times$$

$$\times\left\{\underbrace{(a,0)+(a,0)+\ldots+(a,0)}_{r\text{krát}}+\underbrace{(0,a)+(0,a)+\ldots+(0,a)}_{s\text{krát}}\right\}=(k(r+s)\cdot a,l(r+s)\cdot a)$$

Na druhou stranu máme $(ra,sa)\cdot(ka,la)=(r\cdot(k+l)a,s\cdot(k+l)a)$.

Násobení není komutativní. Na druhou stranu se dá snadno ověřit asociativnost. *R* je tedy nekomutativním okruhem, který má řád p^2.

Na závěr je možné definovat nekomutativní okruh řádu *kp* například jako $O_k \oplus R$ nebo jako $Z_k \oplus R$, kde *R* je právě sestrojený nekomutativní okruh, který má p^2 prvků. Takto definovaný okruh je zřejmě nekomutativní, protože obsahuje podokruh, který je izomorfní s *R*.

Jako příklad nekomutativního okruhu řádu p^2 zvolme $p=2$. Mějme *R*, který obsahuje uspořádané dvojice $(0,0),(u,0),(0,u)$ a (u,u), kde *u* je generátor C_2. Pro stručnost a usnadnění označíme tyto prvky $0,a,b,c$ a získáme tabulky:

⊕	**0**	**a**	**b**	**c**
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

⊗	**0**	**a**	**b**	**c**
0	0	0	0	0
a	0	a	a	0
b	0	b	b	0
c	0	c	c	0

Nekomutativní okruhy řádu 4

Jednou jedinou necyklickou komutativní grupou menšího řádu než je 8 je tzv. Kleinova čtyřgrupa V. To je poslední zbývající případ. Buď *R* okruh s takovouto aditivní grupou. Získáme následující tabulky:

$\oplus$	0	u	v	$u \oplus v$
0	0	u	v	$u \oplus v$
u	u	0	$u \oplus v$	v
v	v	$u \oplus v$	0	u
$u \oplus v$	$u \oplus v$	v	u	0

$\otimes$	0	u	v	$u \oplus v$
0	0	0	0	0
u	0	a_1	a_2	$a_1 \oplus a_2$
v	0	a_3	a_4	$a_3 \oplus a_4$
$u \oplus v$	0	$a_1 \oplus a_3$	$a_2 \oplus a_4$	$a_1 \oplus a_2 \oplus a_3 \oplus a_4$

Okruh *R* definujeme jednoznačně, jestli-že bude zadána každá z hodnot a_1, a_2, a_3, a_4. Budeme tedy značit *R* jako (a_1, a_2, a_3, a_4). Na první pohled, pokud jsou 4 možnosti pro každé a_i, máma tady co činit s 256 případy. Ovšem tento počet se sníží použitím asociativního zákona a zbytek rozdělíme do izomorfních případů. Distributivní zákon nesníží počet případů, protože *R* byl konstruován za předpokladu, že tento zákon bude platit.

POZNÁMKA: Dále budeme pro zápis operací okruhu *R* používat běžné operace sčítání a násobení.

Asociativní zákon $\left[a(bc)=(ab)c, \forall a,b,c \in R\right]$ jistě platí, pokud některý z prvků je 0. Dále také platí-li pro $a,b,c \in \{u,v\}$, potom nejspíše platí obecně. Například mějme případ, kdy $a=u+v, b=u, c=v$, potom

$(u+v)\cdot(uv)=u(uv)+v(uv)$ (distributivní zákon)

$=(uu)v+(vu)v$ (asociativní zákon pro $\{u,v\}$)

$=(uu+vu)\cdot v$ (distributivní zákon)

$=((u+v)\cdot u)\cdot v$ (distributivní zákon)

a proto asociativní zákon platí pro $u+v,u,v$ v tomto pořadí.

Obecný asociativní zákon může být nahrazený následujícími osmi podmínkami:

$u\cdot u\cdot u=u\cdot x_1=x_1\cdot u$ (1) $\quad$ $v\cdot u\cdot u=v\cdot x_1=x_3\cdot u$ (2)

$u\cdot u\cdot v=u\cdot x_2=x_1\cdot v$ (3) $\quad$ $v\cdot u\cdot v=v\cdot x_2=x_3\cdot v$ (4)

$u\cdot v\cdot u=u\cdot x_3=x_2\cdot u$ (5) $\quad$ $v\cdot v\cdot u=v\cdot x_3=x_4\cdot u$ (6)

$u\cdot v\cdot v=u\cdot x_4=x_2\cdot v$ (7) $\quad$ $v\cdot v\cdot v=v\cdot x_4=x_4\cdot v$ (8)

Rozeberme si komutativní a nekomutativní případ zvlášť. Nejprve uvažujme, že *R* je nekomutativní, potom existuje $4\times4\times3\times4=192$ teoretických možností pro x_1,x_2,x_3,x_4, protože zamítáme, aby $vu=x_3$ bylo rovno *uv*. Ovšem pokud $x_1=v$ nebo $x_1=u+v$, potom je *R* komutativní z (1). Proto $x_1=0$ nebo $x_1=u$, a obdobně dostaneme z (8), že $x_4=0$ nebo $x_4=v$. Důsledkem toho zbývá už jen $2\times4\times3\times2=48$ případů.

Dále pokud $x_2=u+v$, potom z (3) $u(u+v)=x_1v$, tedy $x_1+x_2=x_1v$.

Právě jsme tím dokázali, že $x_1 = 0$ nebo $x_1 = u$. To implikuje $x_2 = 0$ nebo $x_1 + x_2 = x_2$, ale oboje nesmí platit. (Podrobně: $x_1 = 0 \Rightarrow x_2 = 0; x_1 = u \Rightarrow u + x_2 = uv, x_1 + x_2 = x_2, x_1 = 0$)

Proto platí, že $x_2 \neq u + v$, a obdobně (ze (6) $x_3 \neq u + v$.

Na závěr, pokud $x_1 = x_4 = 0$, potom z (3) a (7) $\Rightarrow 0 = u \cdot x_2 = x_2 \cdot v$.

Jedním jediným řešením je tedy $x_2 = 0$. (Jako příklad $x_2 = u \Rightarrow 0 = uv \Rightarrow 0 = x_2$, čím se dostáváme ke sporu.)

Zůstalo nám tedy $2 \times 3 \times 2 \times 2 - 1 \times 3 \times 2 \times 1 = 18$ případů. Vzniklou situaci můžeme shrnout takto:

<table>
<tr><td>x1</td><td>0</td><td>u</td><td>u</td></tr>
<tr><td>x2</td><td>v</td><td>0</td><td>v</td></tr>
<tr><td>x3</td><td colspan="3" rowspan="2">Cokoli z trojice 0, u, v,
ale navzájem různé</td></tr>
<tr><td>x4</td></tr>
</table>

Uvažujme tak, že $x_1 = 0$ a $x_4 = v$. Potom z (2) a (3) vyplývá, že $ux_2 = 0 = x_3u$. Pokud by $x_2 = v$ nebo $x_3 = v$, potom bychom dostali okamžitě spor. Zbylé dva možné případy jsou $(0,0,u,v)$ nebo $(0,u,0,v)$. Přičemž oba dva dávají okruh.

Obdobně, pokud $x_1 = u$ a $x_4 = 0$, potom $x_2 \neq u$ ze (7) a $x_3 \neq u$ ze (6). Opět získáme dva okruhy, a to okruh $(u,v,0,0)$ a okruh $(u,0,v,0)$.

Posledních šest případů vychází z toho, že $x_1 = u$ a $x_4 = v$. Rovnosti (4) a (5) jsou následující: $vx_2 = x_3v$ a $ux_3 = x_2u$. Pokud položíme $x_2 = 0$, potom se zredukují tyto rovnosti na $x_3v = 0 = ux_3$. Proto jediná možnost řešení je $x_3 = 0$, ale ta nemůže nikdy nastat, protože *R* je nekomutativní okruh. Obdobně $x_3 = 0$ dává spor.

Zbývají tedy možnosti (u,u,v,v) a (u,v,u,v), které nám dají okruhy.

Izomorfní okruhy řádu 4

Každý okruhový izomorfismus je také zároveň izomorfismem odpovídajících si aditivních grup těchto okruhů. Grupový izomorfismus Kleinovy grupy musí být ve tvaru permutace na tříprvkové množině *u, v,* $u+v=w$. Jak už je ve zvyku, budeme těchto šest permutací zapisovat do tvaru cyklů: *Id* (identita), $(u,v),(v,w),(w,\mathrm{u}),(u,v,w),\ (u,w,v)$.

Uvažujme, že (x_1,x_2,x_3,x_4) je okruhem *R* řádu 4 a nechť φ je okruhovým izomorfismem *R* na *R*. Pak pro každé x_i zobrazení na $\varphi(x_i)$ pro $i=1,2,3,4$. V tomto okamžiku můžeme určit čtveřice, které dávají charakterizaci okruhu, který je obrazem původního okruhu při shora uvedeném izomorfismu.

Například mějme $\varphi=(w,u)$. Potom $\varphi(u)=w$, $\varphi(\mathrm{v})=v$ a $\varphi(w)=u$. Sestavíme tabulku multiplikativního zobrazení φ:

	$\varphi(0)$	$\varphi(\mathrm{u})$	$\varphi(\mathrm{v})$	$\varphi(w)$
$\varphi(0)$	$\varphi(0)$	$\varphi(0)$	$\varphi(0)$	$\varphi(0)$
$\varphi(\mathrm{u})$	$\varphi(0)$	$\varphi(x_1)$	$\varphi(x_2)$	$\varphi(x_1+x_2)$
$\varphi(\mathrm{v})$	$\varphi(0)$	$\varphi(x_3)$	$\varphi(x_4)$	$\varphi(x_3+x_4)$
$\varphi(w)$	$\varphi(0)$	$\varphi(x_1+x_3)$	$\varphi(x_2+x_4)$	$\varphi(x_1+x_2+x_3+x_4)$

Po dosazení odpovídajících sis hodnot a po úpravě získáváme:

	0	$u + v$	v	u
0	0	0	0	0
$u + v$	0	$\varphi(x_1)$	$\varphi(x_2)$	$\varphi(x_1)+\varphi(x_2)$
v	0	$\varphi(x_3)$	$\varphi(x_4)$	$\varphi(x_3)+\varphi(x_4)$
u	0	$\varphi(x_1)+\varphi(x_3)$	$\varphi(x_2)+\varphi(x_4)$	$\varphi(x_1)+\varphi(x)_2+\varphi(x_3)+\varphi(x_4)$

Pokud tabulku uspořádáme běžným způsobem, získáme následující výsledek:

	0	u	v	$u + v$
0	0	0	0	0
u	0	$\varphi(x_1)+\varphi(x)_2+\varphi(x_3)+\varphi(x_4)$	$\varphi(x_2)+\varphi(x_4)$	$\varphi(x_1)+\varphi(x_3)$
v	0	$\varphi(x_3)+\varphi(x_4)$	$\varphi(x_4)$	$\varphi(x_3)$
$u + v$	0	$\varphi(x_1)+\varphi(x_2)$	$\varphi(x_2)$	$\varphi(x_1)$

Okruh je určen čtveřicí $(\varphi(x_1)+\varphi(x)_2+\varphi(x_3)+\varphi(x_4), \varphi(x)_2+\varphi(x_4), \varphi(x_3)+\varphi(x_4), \varphi(x_4))$.
Uvažujme, že máme okruh *R*, který bude určen čtveřicí (u,v,u,v). Potom za pomoci izomorfismu (w,u) získáme $(w+v+w+v, v+v, w+v, v)$, což znamená, že $(u,v,u,v)\cong(0,0,\mathrm{u},\mathrm{v})$. Výše uvedeným způsobem lze určit obrazy okruhů při izomorfismech těmito permutacemi:

Identita $(\varphi(x_1),\varphi(x_2),\varphi(x_3),\varphi(x_4))$

(u,v) $(\varphi(x_4),\varphi(x_3),\varphi(x_2),\varphi(x_1))$

(v,w) $(\varphi(x_1),\varphi(x_1)+\varphi(x_2),\varphi(x_1)+\varphi(x_3),\varphi(x_1)+\varphi(x_2)+\varphi(x_3)+\varphi(x_4))$

(w,u) $\quad (\varphi(x_1)+\varphi(x_2)+\varphi(x_3)+\varphi(x_4),\varphi(x_2)+\varphi(x_4),\varphi(x_3)+\varphi(x_4),\varphi(x_4))$

(u,v,w) $\quad (\varphi(x_1)+\varphi(x_2)+\varphi(x_3)+\varphi(x_4),\varphi(x_1)+\varphi(x_3),\varphi(x_1)+\varphi(x_2),\varphi(x_1))$

(u,w,v) $\quad (\varphi(x_4),\varphi(x_3)+\varphi(x_4),\varphi(x_2)+\varphi(x_4),(\varphi(x_1)+\varphi(x_2)+\varphi(x_3)+\varphi(x_4))$

Odtud můžeme nahlédnout, že:

$(u,v,u,v)\cong(0,0,u,v)$ [bylo užito (w,u)]

$\cong(u,v,0,0)$ [bylo užito (v,w)]

$(u,u,v,v)\cong(0,u,0,v)$ [bylo užito (w,u)]

$\cong(u,0,v,0)$ [bylo užito (v,w)]

To znamená, že až na izomorfismus, existují pouze dva nekomutativní okruhy řádu 4, a to (u,v,u,v) a (u,u,v,v). Každý z těchto okruhů obsahuje jednostranný jednotkový prvek, ale neobsahuje oboustrannou jednotku.

Komutativní okruhy řádu 4

Pokud položíme $x^3=x^2$, potom dostáváme komutativní okruh ve tvaru (x_1,x_2,x_3,x_4) a asociativní zákon nám poskytne dvě podmínky: $u\cdot x_2=x_1\cdot v$ a $x_4=x_2\cdot v$. Nejprve uvažujme, že okruh *R* má jednotku, například *u*. Potom platí $x_1=u$, $x_2=v$ a asociativní zákony. Proto každá ze čtyř možných hodnot pro x_4 nám dá okruh:

$x_4=0$: dává obor integrity hlavních ideálů, proto tedy v tomto okruhu můžeme jakýkoli ideál generovat jediným prvkem.

$x_4=u$: dává stejný obor hlavních ideálů, protože $(u,v,v,0)\cong(u,v,v,u)$ - izomorfismus (v,w).

$x_4=v$: ten nám dá $Z_2\oplus Z_2$, jiný obor integrity hlavních ideálů.

$x_4=u+v$: dává *GF*(4), což je Galoisovo těleso řádu 4

Na závěr uvažujme, že okruh nebude mít jednotku. Potom není ve tvaru: (u,v,v,x_4) s jednotkou u, (x_1,u,u,v) s jednotkou v, ale ani $(u+x,x,x,v+x)$ s jednotkou $u+v$.

Mějme $x_1=0$, potom z asociativního zákona platí, že $u\cdot x_2=0$, což implikuje $x_1\neq v$, $u+v$ a $u\cdot x_4=x_1\cdot v$. Pokud $x_2=u$, potom jediná možná řešení jsou $x_4=v$ nebo $x_4=u+v$, což ale vylučujeme, protože jsme si dali předpoklad, že okruh nemá jednotkový prvek. Tím pádem jsme opustili okruhy ve tvaru $(0,0,0,x_4)$.

Obdobně:

$x_1=u$ dává $(u,0,0,0)$ a (u,u,u,u)

$x_1=v$ dává $(v,0,0,0)$ a (v,v,v,v)

$x_1=u+v$ dává $(u+v,0,0,0)$ a $(u+v,u+v,u+v,u+v)$.

Pokud použijeme předchozí výsledky o izomorfismu, dokážeme tuto množinu rozdělit do následujících tříd navzájem izomorfních okruhů:

a) $(0,0,0,0)$, triviální okruh $O_2\oplus O_2$

b) $(0,0,0,u)\cong(v,0,0,0)$ (izomorfismus (u,v))
$\cong(u+v,u+v,u+v,u+v)$ (izomorfismus (w,u))

c) $(0,0,0,v)\cong(u,0,0,0)$ (izomorfismus (u,v))
$\cong(0,0,0,u+v)$ (izomorfismus (v,w))
$\cong(v,v,v,v)$ (izomorfismus (w,u))
$\cong(u+v,0,0,0)$ (izomorfismus (u,v,w))
$\cong(u,u,u,u)$ (izomorfismus (u,w,v))

Třetí okruh $(0,0,0,v)$ můžeme ztotožnit $(u\leftrightarrow(0,1),v\leftrightarrow(0,1))$ s okruhem $Z_2\oplus O_2$.

Závěr okruhů

V tuto chvíli můžeme vypsat seznam všech asociativních okruhů až do řádu 7 (včetně). Tento seznam uvedeme pro přehlednost v následující tabulce:

Řád	**Okruh**	**Aditivní grupa**	**Vlastnosti**
1	O_1	C_1	Komutativní okruh
2	O_2	C_2	Komutativní okruh
2	Z_2	C_2	Komutativní těleso
3	O_3	C_3	Komutativní okruh
3	Z_3	C_3	Komutativní těleso
4	O_4	C_4	Komutativní okruh
4	Z_4	C_4	Okruh hl. ideálů
4	$„u^2 = 2u“$	C_4	Komutativní okruh
4	(u, v, u, v)	V	Nekomut. okruh s levou 1
4	(u, u, v, v)	V	Nekomut. okruh s pravou 1
4	$Z_2 \oplus Z_2$	V	Okruh hl. ideálů
4	$GF(4)$	V	Komutativní těleso
4	$(u, v, v,0)$	V	Okruh hl. ideálů
4	$O_2 \oplus O_2$	V	Komutativní okruh
4	$Z_2 \oplus O_2$	V	Komutativní okruh
5	O_5	C_5	Komutativní okruh

5	Z_5	C_5	Těleso
6	O_6	C_6	Komutativní okruh
6	Z_6	C_6	Okruh hl. ideálů
6	$Z_3 \oplus O_2$	C_6	Komutativní okruh
6	$Z_2 \oplus O_3$	C_6	Komutativní okruh
7	O_7	C_7	Komutativní okruh
7	Z_7	C_7	Komutativní těleso

V části věnované okruhům i v uvedené tabulce jsme přejali dohodu, že okruh hlavních ideálů má jednotkový prvek. Nejmenším z těles je Z_2 a ten je také nejmenším euklidovským oborem integrity, oborem integrity hlavních ideálů a oborem integrity s jednoznačným rozkladem. Protože každý konečný obor integrity je tělesem, nemá význam hledat nejmenší konečný obor integrity, který není oborem integrity s jednoznačným rozkladem atd.

Na závěr si všimněme, že nejmenší nekomutativní okruh je řádu 4. Nemůže jít o obor, protože konečný okruh bez dělitelů nuly je okruhem s dělením (to znamená nekomutativním tělesem) a každý konečný okruh s dělením je podle Wedderburnovy věty tělesem komutativním.

Závěr

Cílem této diplomové práce bylo podat ucelený přehled základních informací o okruzích s malým počtem prvků. Také jsme zde shrnuli základní vlastnosti další konečné algebraické struktury malých řádů, a to struktury grup. Zopakovali jsme zde některé pojmy, které jsou potřebné k rozvoji teorie, uvedli jsme platnost základních tvrzení o těchto strukturách a doplnili je o důkazy platnosti těchto tvrzení.

K popisování jednotlivých grup jsme využívali především operační tabulky, které sloužili k přehlednosti, protože pouhý zápis výsledků jednotlivých operací by byl nepřehledný a čtenář by se v něm mohl snadno ztratit. Povedlo se nám popsat všechny grupy řádu maximálně 15 (až na izomorfismus), a to jak komutativní, tak i nekomutativní. Počty jednotlivých existujících grup jednotlivých řádů jsme shrnuli do tabulky v závěru části, která se věnovala teorii grup. Velmi zajímavým a cenným je poznatek o způsobu konstrukce grup za pomoci direktního součinu. K tvorbě grup vyšších řádů napomáhají hlavně Sylowovy věty.

V teorii okruhů jsme provedli klasifikaci všech asociativních okruhů řádů menších nebo rovných 7 na základě aditivních grup. V práci jsou uvedeny jednotlivé druhy okruhů, ať už jde o komutativní nebo nekomutativní okruhy, izomorfní okruhy, anebo okruhy s cyklickou aditivní grupou.

Resumé

As the title suggests, this work focuses on circuits with a small number of elements. This diploma thesis deals with the topic of finite algebraic structures (namely, small-order circuits, but also contains a topic related to the group). Only in colleges students will learn in detail in various lessons (seminars and lectures) with different algebraic structures, either with one or even two operations. It is clear that groups, circuits, and other algebraic structures are built from simpler to more complex structures. This also implies the importance of finite structures of small orders. It is also clear that these structures serve students to understand and gain an understanding of the substance being studied. The knowledge of these examples helps students to get a concrete idea of the theory under discussion, and the students are equipped with simple examples of structure. They can help students understand the definitions and sentences that will follow in developing the theory. But it is true that some of the structures can be met by primary school pupils without knowing that they are working with such things.

This work builds on the knowledge that students obtain from algebra classes and summarizes the basic properties of finite groups of small orders and finite circles of small orders. At the same time, in group theory, we will familiarize with Sylow's sentences, which are very important.

Seznam literatury

[1] Fletcher C. R., Ring sof small order, The Mathematical Gazette, Vol.64, No.427 9-22, March 1980

[2] Bican, L.: Algebra I, SPN, Praha 1979. Skriptum MFF UK Praha.

[3] Bicanová A., Kepka, T. Nováková, E.: Sbírka úloh, příkladů a cvičení z algebry, SPN, Praha 1984. Skriptum MFF UK Praha.

[4] Procházka, L. a kol.: Algebra, Academia, Praha, 1990

[5] HORA, Jaroslav. *Algebra I: Určeno posl. 4. roč. učitelství VVP [všeobecně vzdělávací předměty]*. 1. vyd. Plzeň: Pedagogická fakulta, 1991. 111 s. Učební texty vysokých škol. ISBN 80-7043-030-3

[6] BURIAN, Květoslav a LIBICHER, Jaroslav. *Algebra. 1*. Ostrava: Pedagogická fakulta v Ostravě, [1977]. 167 s.

[7] BLAŽEK, Jaroslav et al. *Algebra a teoretická aritmetika: Celost. a vysokošk. učebnice pro stud. matematicko-fyzikálních, přírodověd. a pedagog. fakult. Díl 2*. 1. vyd. Praha: SPN, 1985. 258 s. Učebnice pro vysoké školy

[8] BŘACHOVÁ, Kateřina. *Konečné algebraické struktury*. Plzeň, 1996. Diplomová práce. ZČU v Plzni. Vedoucí práce doc. RNDr. Jaroslav Hora, CSc.

[9] ŠELLEROVÁ, Lenka. *Řešené úlohy z obecné algebry*. Plzeň, 2014. Bakalářská práce. ZČU v Plzni. Vedoucí práce doc. RNDr. Jaroslav Hora, CSc. Dostupné z: https://otik.uk.zcu.cz/bitstream/11025/13022/1/Bakalarska%20prace.pdf

Seznam tabulek