ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

KONEČNÉ GRUPY MALÝCH ŘÁDŮ

BAKALÁŘSKÁ PRÁCE

Magda Bláhová

Matematika se zaměřením na vzdělávání (maior) + Technická výchova se zaměřením na vzdělávání (minor)

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

Plzeň, 2023

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

V Plzni, 20. června 2023

.....

vlastnoruční podpis

Tímto bych chtěla poděkovat mému vedoucímu bakalářské práce, doc. RNDr. Jaroslavu Horovi, CSc., za pomoc a cenné rady v průběhu jejího zpracování.

OBSAH

ÚVOD 2

1 BINÁRNÍ OPERACE A ALGEBRAICKÉ STRUKTURY 3

1.1 VLASTNOSTI A VÝZNAMNÉ PRVKY BINÁRNÍCH OPERACÍ 3

2 GRUPY, POLOGRUPY A DALŠÍ STRUKTURY 6

3 GRUPY SYMETRIÍ GEOMETRICKÝCH OBRAZCŮ 16

3.1 OBDÉLNÍK 16

3.2 ROVNOSTRANNÝ TROJÚHELNÍK 18

3.3 ČTVEREC 19

3.4 PRAVIDELNÝ PĚTIÚHELNÍK 21

3.5 PRAVIDELNÝ N-ÚHELNÍK 23

4 HOMOMORFISMUS A IZOMORFISMUS GRUP 24

5 KONEČNÉ GRUPY MALÝCH ŘÁDŮ 28

5.1 GRUPY PRVOČÍSELNÝCH ŘÁDŮ 28

5.2 KOMUTATIVNÍ GRUPY NEPRVOČÍSELNÝCH ŘÁDŮ 36

5.3 NEKOMUTATIVNÍ GRUPY NEPRVOČÍSELNÝCH ŘÁDŮ 44

ZÁVĚR 55

RESUMÉ 56

SEZNAM LITERATURY 57

SEZNAM OBRÁZKŮ, TABULEK, GRAFŮ A DIAGRAMŮ 59

ÚVOD

Práce konečné grupy malých řádů se zabývá grupami, jejichž řád je maximálně 15. Řád určuje počet prvků, které daná grupa má. Svou práci jsem rozdělila do pěti kapitol.

První z nich se věnuje binárním operacím a algebraickým strukturám. Ty tvoří úplný základ, bez něhož by nebylo možné grupy zkoumat.

Druhá kapitola se již věnuje grupám a dalším strukturám a zavádí konkrétní algebraické struktury včetně jejich vlastností a příkladů. Objevuje se zde také několik definic a vět, které jsou potřebné pro další studium grup.

Následující třetí kapitola se zabývá grupami symetrií geometrických obrazců. Rozebírá základní geometrické obrazce se všemi jejich symetriemi a skládáním.

Kapitola čtvrtá se věnuje homomorfismu a izomorfismu grup, jakožto důležitým zobrazením mezi algebraickými strukturami. Opět v ní nechybí ani řada vět a definic, které umožňují snadnější zkoumání.

Poslední kapitola pak nese název shodný s názvem práce a zaměřuje se na konečné grupy malých řádů. Ty se dále dělí ještě na grupy komutativní a nekomutativní. Nachází se zde způsoby, jak tyto grupy najít, ale i sestrojené operační tabulky.

1 BINÁRNÍ OPERACE A ALGEBRAICKÉ STRUKTURY

Pro definici grup jsou nezbytně nutné binární operace, jejich základní vlastnosti a algebraické struktury. Proto se budeme v první kapitole věnovat právě jim.

Definice 1.1: Binární operace

Binární operace * na množině M je zobrazení z kartézského součinu $M \times M$ do M. Symbolicky ji můžeme zapsat jako $*: M \times M \to M$.

Vstupní hodnoty v binární operaci nazýváme operandy. Této dvojici prvků kartézského součinu $(a, b) \in M$ operace přiřazuje jediný prvek $c \in M$, který je pak výsledkem zadané operace.

Příkladem může být třeba binární operace plus (+), která prvkům $a = 3$ a $b = 5$ přiřadí prvek $c = 8$, symbolicky bychom ji zapsali jako $+: [3, 5] \to 8$.

Právě sčítání je jednou z běžných binárních operací na množině celých čísel, stejně jako třeba násobení či odčítání, dělení však nikoli, protože může dát zlomek. U čísel přirozených můžeme sčítat a násobit, ale ne dělit ani odčítat, neboť z dělení můžeme dostat zlomek a z odčítání kladných čísel může vzejít číslo záporné.

1.1 Vlastnosti a významné prvky binárních operací

Definice 1.2: Komutativita

Operace * je na množině M komutativní, pokud u ní platí, že:

$(\forall a, b \in M): a * b = b * a$.

Tato vlastnost nám říká, že nezáleží na pořadí prvků. U základních operací je komutativní sčítání a násobení, nekomutativní pak odčítání a dělení. Z dalších operací je komutativní např. sjednocení a průnik množin nebo sčítání vektorů.

Definice 1.3: Asociativita

Operace * je na množině M asociativní, pokud u ní platí, že:

$(\forall a, b, c \in M): (a * b) * c = a * (b * c)$.

Zde nám jde o přednosti operací, které udávají závorky. Obecně tuto vlastnost stejně jako vlastnosti předchozí splňuje sčítání a násobení, odčítání a dělení nikoli. Opět sem ale patří i sjednocení a průnik množin či sčítání vektorů.

Definice 1.4: Neutrální prvek

Prvek e nazýváme neutrálním (nebo také jednotkovým), pokud u dané binární operace * na množině M platí, že:

$(\forall a \in M)\ (\exists e \in M)$: $a * e = e * a = a$.

Neutrálním prvkem je tedy prvek, který v dané operace s jakýmkoli jiným prvkem zachovává jeho hodnotu, tedy nám vlastně operování s neutrálním prvkem vůbec nic nemění. Intuitivně je tedy nula neutrálním prvkem u operace sčítání a jednička u operace násobení. U odčítání a dělení můžeme tyto prvky využít také, ale nebude nám to platit oboustranně, neboť tyto operace nejsou komutativní. Odtud plyne další rozdělení neutrálních prvků:

Definice 1.4 (a): Levý neutrální prvek

Prvek e nazýváme levým neutrálním, jestliže něj platí pouze následující tvrzení:

$(\forall a \in M)\ (\exists e \in M)$: $e * a = a$.

Definice 1.4 (b): Pravý neutrální prvek

Prvek e nazýváme pravým neutrálním, jestliže u něj platí pouze následující tvrzení:

$(\forall a \in M)\ (\exists e \in M)$: $a * e = a$.

Nyní již můžeme říct, že nula je pravým neutrálním prvkem u operace odčítání a jednička pravým neutrálním prvkem u operace dělení.

Definice 1.5: Inverzní prvek

Prvek a^{-1} nazýváme inverzním prvkem k prvku a v binární operaci * na množině M, jestliže platí:

$a * a^{-1} = a^{-1} * a = e$, kde e značí neutrální prvek operace *.

Jedná se tedy o prvek, který v zadané operaci s původním prvkem dá prvek neutrální. U sčítání a odčítání proto získáme inverzní prvek záměnou znaménka, u násobení převrácenou hodnotou a u dělení je prvek inverzní sám sobě.

Definice 1.6: Agresivní prvek

Prvek g nazýváme agresivním, jestliže u zadané binární operace * na množině M platí:

$(\forall a \in M)$: $a * g = g * a = g$.

Jedná se tedy o prvek, který v kombinaci s čímkoli dá ve výsledku sám sebe. Intuitivně je nula agresivním prvek u operace násobení. Obdobně jako u inverzních prvků může i agresivní prvek platit pouze jednostranně:

Definice 1.6 (a): Levý agresivní prvek

Prvek g nazýváme levým agresivním, jestliže u něj platí pouze následující tvrzení:
$(\exists a \in M): g * a = g.$

Definice 1.6 (b): Pravý agresivní prvek

Prvek g nazýváme pravým agresivním, jestliže u něj platí pouze následující tvrzení:
$(\exists a \in M): a * g = g.$
Příkladem může být opět číslo 0, které je levým agresivním prvkem u operace dělení.

Definice 1.7. Algebraická struktura

Algebraickými strukturami nazýváme množiny, na nichž je definována alespoň jedna binární operace. Množiny musí být v kombinaci s danými operacemi uzavřené. Symbolicky je značíme jako (M, *).
Příklady algebraických struktur

- (N, *): operace násobení na množině přirozených čísel
- (N, +): operací sčítání na množině přirozených čísel
- (Z, –): operace odčítání na množině celých čísel
- (Q, /): operace dělení na množině racionálních čísel
- (V, +): operace sčítání na množině vektorů

2 GRUPY, POLOGRUPY A DALŠÍ STRUKTURY

Pojem grupa jako první použil francouzský matematik Évariste Galois (1811–1832). Stal se proto jedním ze zakladatelů dnešní teorie grup. Jeho prvotním záměrem však bylo řešení polynomiálních rovnic vyšších stupňů.

Definice 2.1: Grupa

Grupou nazýváme algebraickou strukturu (M, *), jejíž operace * splňuje několik axiomů:

- je asociativní: $(\forall a, b, c \in M)$: $a * (b * c) = (a * b) * c$,
- má neutrální prvek: $(\forall a \in M)$: $a * e = e * a = a$,
- každý její prvek má prvek inverzní: $a * a^{-1} = a^{-1} * a = e$.

Příklady grup

- $(Z, +)$: operace sčítání na množině celých čísel
- $(Q, \cdot)$: operace násobení na množině racionálních čísel
- $(Z_n, +)$: operace sčítání na množině celých čísel modulo n
- $(Z_n^*, \cdot)$: operace násobení na množině celých čísel modulo n bez nuly, kde n je prvočíslo
- triviální grupa, tedy grupa, která obsahuje pouze jediný prvek, a to e (prvek neutrální)

Příklad 2.1

Budeme-li mít například grupu $(Z_5, \cdot)$, tedy násobení na množině celých čísel modulo 5, pak bude operační tabulka vypadat následovně:

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabulka 1: Operační tabulka násobení na množině Z_5

Chceme-li ověřit, že je daná struktura skutečně grupou, ověříme postupně všechny podmínky:

1) Asociativita: operace zjevně je asociativní, neboť máme operaci násobení, u které nikdy nezáleží na pořadí, v jakém ho provádíme.
2) Neutrální prvek: můžeme si všimnout, že první řádek i první sloupec kopírují záhlaví tabulky. Z toho vyplývá, že tato struktura má neutrální prvek a je jím jednička.
3) Inverzní prvky: opět se můžeme podívat do tabulky – v každém řádku i každém sloupci se všechna čísla vyskytují právě jednou, a to i jednička, tedy neutrální prvek. Všechny prvky proto mají prvky inverzní (jednička je inverzní sama sobě, pro dvojku je inverzní prvkem trojka a pro trojku dvojka, čtyřka je opět inverzní sama sobě).

Všechny tři nutné podmínky máme splněné, tedy můžeme říct, že tato algebraická struktura skutečně je grupou.

Definice 2.2: Abelovská neboli komutativní grupa

Algebraickou strukturu (M, *) nazýváme abelovskou grupou, pokud u její operace * kromě axiomů pro grupu platí také komutativita:

$(\forall a, b \in M): a * b = b * a.$

Příklady komutativních grup

- Struktury uvedené u grup jsou zjevně i grupami komutativními.
- Totéž platí i pro příklad 2.1, neboť v tabulce můžeme snadno vidět, že je souměrná podle hlavní diagonály, tedy pro všechny prvky platí, že $a * b = b * a$, a proto daná grupa je komutativní.

Definice 2.3: Pologrupa

Pologrupou nazýváme algebraickou strukturu (M, *), jejíž operace * splňuje axiom asociativity:

$(\forall a, b, c \in M): (a * b) * c = a * (b * c).$

Příklady pologrup

- (N, +): operace sčítání na množině přirozených čísel
- (Z, +): operace sčítání na množině celých čísel

- (N, ·): operace násobení na množině přirozených čísel
- (Z, ·): operace násobení na množině celých čísel
- (Z, –): operace odčítání na množině celých čísel

Definice 2.4: Abelovská neboli komutativní pologrupa

Algebraickou strukturu (M, *) nazýváme abelovskou pologrupou, pokud u její operace * kromě axiomů pro pologrupu platí také komutativita:

$(\forall a, b \in M): a * b = b * a.$

Příklady komutativních pologrup

- Mimo odčítání jsou struktury uvedené u pologrup zjevně i komutativní.

Definice 2.5: Monoid neboli pologrupa s neutrálním prvkem

Monoidem nazýváme algebraickou strukturu (M, *), která je pologrupou a zároveň u ní platí axiom existence neutrálního prvku:

$(\forall a \in M)\ (\exists e \in M): a * e = e * a = a.$

Příklady monoidů

- (Z, +): operace sčítání na množině celých čísel
- (Z, –): operace odčítání na množině celých čísel
- (N, *): operace násobení na množině přirozených čísel

Definice 2.6: Abelovský neboli komutativní monoid

Algebraickou strukturu (M, *) nazýváme abelovský monoid, pokud u její operace * kromě axiomů pro monoid platí také komutativita:

$(\forall a, b \in M): a * b = b * a.$

Příklady komutativních monoidů

- (N, +): operace sčítání na množině přirozených čísel
- (Z, +): operace sčítání na množině celých čísel
- (Z, *): operace násobení na množině celých čísel

Definice 2.7: Grupoid

Grupoidem nazýváme algebraickou strukturu (M, *), která kromě uzavřenosti nemusí splňovat žádné speciální předpoklady.

Příklady grupoidů

- (N, +): operace sčítání na množině přirozených čísel
- (Z, –): operace odčítání na množině celých čísel
- (N, ·): operace násobení na množině přirozených čísel

Definice 2.8: Abelovský neboli komutativní grupoid

Algebraickou strukturu (M, *) nazýváme abelovský grupoid, pokud u její operace * kromě axiomů pro grupoid platí také komutativita:

$(\forall a, b \in M)$: $a * b = b * a$.

Příklady komutativních grupoidů

- (N, +): operace sčítání na množině přirozených čísel
- (Z, +): operace sčítání na množině celých čísel
- (N, ·): operace násobení na množině přirozených čísel

Vlastnosti jednotlivých algebraických struktur můžeme vyjádřit také tabulkou:

	Asociativita	Komutativita	Neutrální prvek	Inverzní prvky
Grupa	ano	ne	ano	ano
Abelovská grupa	ano	ano	ano	ano
Pologrupa	ano	ne	ne	ne
Abelovská pologrupa	ano	ano	ne	ne
Monoid	ano	ne	ano	ne
Abelovský monoid	ano	ano	ano	ne
Grupoid	ne	ne	ne	ne
Abelovský grupoid	ne	ano	ne	ne

Tabulka 2: Přehled vlastností jednotlivých algebraických struktur

Z tabulky můžeme vidět, že každá grupa je zároveň i monoidem, pologrupou nebo grupoidem. Totéž platí i pro komutativní grupu, která je také komutativním monoidem, komutativní pologrupou i komutativním grupoidem.
Struktury, které v tabulce uvedené nejsou, můžeme pojmenovávat jednoduše přidáním odpovídající vlastnosti, například grupoid s neutrálním prvkem.

Niels Henrik Abel

Abelovské algebraické struktury nesou své jméno po norském matematikovi Nielsovi Henriku Abelovi. Ten se narodil v roce 1802 v Nedstrandu a zemřel v necelých 27 letech roku 1829 ve Frolandu. Jeho matematického talentu si všiml již učitel na katedrální škole a motivoval ho studovat matematiku na vyšší úrovni.

Obrázek 1: Niels Henrik Abel [20]

Už v době, kdy v roce 1821 nastoupil na univerzitu, byl velmi zkušeným matematikem. Začal se věnovat jednomu z otevřených matematických problémů, který se týkal neřešitelnost kvintických rovnic (5. stupně) a vyšších pomocí obecných vzorců, díky nimž můžeme řešit rovnice nižších stupňů. Dokázat tuto neřešitelnost se mu skutečně povedlo, ačkoli zprvu nikdo nevěřil tomu, že to tak mladičký student

mohl opravdu zvládnout. Promoval pak hned rok po tom, co na univerzitu nastoupil, v roce 1822.

Později se začal věnovat také eliptickým funkcím a objevil i funkce abelovské, což jsou periodické funkce komplexních proměnných. Díky mnoha darům specialistů mohl cestovat po spoustě zemí, učit se jazyky a publikovat v matematice. Většina jeho prací končila v Berlíně, kde ho také měli na univerzitě v roce 1829 jmenovat profesorem. Toho už se ale nedožil, ani se o tom nedozvěděl, neboť se nakazil tuberkulózou a zemřel.

Na jeho počest byla již v roce 1899 navržena Abelova cena, která měla být doplňkem k cenám Nobelovým. Opravdu zavedena však byla až v roce 2002, tedy 200 let po narození Abela. Udělena pak poprvé byla v roce 2003, norský král jí oceňuje vynikající matematiky.

Definice 2.9: Podgrupa

Grupu (N, **) nazveme podgrupou grupy (M, *), pokud platí, že množina N je podmnožinou množiny M a zároveň podgrupa (N, **) je asociativní a má neutrální prvek i prvky inverzní, tedy je sama grupou. Také platí, že každá grupa je sama sobě podgrupou.

$\langle g \rangle$ značí podgrupu generovanou prvkem g. Jedná se tedy o množinu, v níž jsou všechny mocniny g, inverzní prvky a jednotkový prvek.

Podgrupy dále můžeme dělit na nevlastní, které jsou dvě – grupa sama a její triviální podgrupa, která obsahuje jen neutrální prvek, a vlastní, což jsou všechny ostatní podgrupy.

Definice 2.10: Cyklická grupa

Grupu M nazýváme cyklickou, pokud existuje prvek $g \in M$ takový, že $M = \langle g \rangle$, tento prvek nazýváme generátorem grupy M.

Příklady cyklických grup

- $(Z_7, +)$: operace sčítání na množině celých čísel modulo 7 (obecně jakékoli sčítání modulo n, kde n je prvočíslo)
- $(Z, -)$: operace odčítání na množině celých čísel

Věta 2.1

Každá cyklická grupa je grupou komutativní.

Důkaz: Každá cyklická grupa má nějaký svůj generátor. Všechny její prvky pak můžeme vyjádřit jako mocninu tohoto generátoru. Na pořadí mocnin však nezáleží – mějme prvky a, b a generátor g. Můžeme zapsat, že $a \cdot b = g^x \cdot g^y = g^{x+y} = g^{y+x} = g^y \cdot g^x = b \cdot a$, tedy $ab = ba$, takže komutativita platí.

Příklad 2.2

Mějme grupu $(Z_7, +)$, tedy operaci sčítání na množině celých čísel modulo 7. Jelikož nás zajímají zbytkové třídy po dělení sedmičkou, máme zde prvky 0, 1, 2, 3, 4, 5, 6. Vezměme si je postupně:

- Nula nemůže být generátorem, neboť nikdy nevygeneruje jiné číslo než nulu. Je úplně jedno, kolik nul sečteme, výsledek bude vždy nulový.
- Jednička generátorem určitě být může, protože zvládne vygenerovat veškeré prvky, které do této množiny patří:
  - $1^1 = 1$
  - $1^2 = 1 + 1 = 2$ (sčítáme, neboť máme v grupě zadanou operaci sčítání)
  - $1^3 = 1 + 1 + 1 = 3$
  - $1^4 = 1 + 1 + 1 + 1 = 4$
  - $1^5 = 1 + 1 + 1 + 1 + 1 = 5$
  - $1^6 = 1 + 1 + 1 + 1 + 1 + 1 = 6$
  - $1^7 = 1 + 1 + 1 + 1 + 1 + 1 + 1 = 0$ (7 modulo 7)
- Totéž můžeme provést i s číslem 2, i to pro nás bude generátorem, neboť s ním dokážeme vygenerovat celou množinu
  - $2^1 = 2$
  - $2^2 = 2 + 2 = 4$
  - $2^3 = 2 + 2 + 2 = 6$
  - $2^4 = 2 + 2 + 2 + 2 = 1$ (8 modulo 7)
  - $2^5 = 2 + 2 + 2 + 2 + 2 = 3$ (10 modulo 7)
  - $2^6 = 2 + 2 + 2 + 2 + 2 + 2 = 5$ (12 modulo 7)
  - $2^7 = 2 + 2 + 2 + 2 + 2 + 2 + 2 = 0$ (14 modulo 7)

- Snadno bychom se přesvědčili, že generátory této množiny mohou být i všechna další čísla (3, 4, 5, 6), která do ní patří, neboť jejich sčítáním a operací modulo 7 můžeme vždycky vygenerovat celou množinu. Toto platí u všech Z_n, kde n je prvočíslo – generátory jsou všechny nenulové prvky.

Příklad 2.3

Vezměme grupu $(Z_4, +)$, tedy opět grupu se sčítáním, ale tentokrát modulo 4, což není prvočíslo. Opět si projdeme postupně jednotlivé prvky:

- Nula ani tady není generátorem, neboť ostatní prvky nevygeneruje.
- Jednička generátorem bude, neboť zde platí totéž, co v předchozím příkladu.
- Číslo dvě bude vypadat následovně:
  - $2^1 = 2$
  - $2^2 = 2 + 2 = 0$ (4 modulo 4)
  - $2^3 = 2 + 2 + 2 = 2$ (6 modulo 4)
  - $2^4 = 2 + 2 + 2 + 2 = 0$ (8 modulo 4)
  - $2^5 = 2 + 2 + 2 + 2 + 2 = 2$ (10 modulo 4)
  - Již nyní můžeme vidět, že se nám ve výsledcích pouze střídají nuly a jedničky. Dvojka nám tedy dokázala vygenerovat nulu, ovšem čísla 1 a 3 nikoliv, neboť sčítáním sudých dvojek nikdy nemůžeme získat lichá čísla. Dvojka tedy není generátorem této množiny.
- Trojka ale opět generátorem bude, neboť snadno nahlédneme, že opravdu vygeneruje celou množinu:
  - $3^1 = 3$
  - $3^2 = 3 + 3 = 2$ (6 modulo 4)
  - $3^3 = 3 + 3 + 3 = 1$ (9 modulo 4)
  - $3^4 = 3 + 3 + 3 + 3 = 0$ (12 modulo 4)
- Můžeme tedy vidět, že máme-li Z_n, kde n není prvočíslo, tak prvků, které nejsou generátory, je víc – kromě nuly to jsou také dělitelé n (mimo jedničky).

Věta 2.2

Grupa je cyklická, když se skládá z mocnin svého generátoru, tedy v ní platí, že:

$M = \langle g \rangle = \{g^k; k \in Z\}$.

Důkaz: Z definice 2.10 víme, že grupa je cyklická, pokud obsahuje nějaký svůj generátor. Prvek nazýváme generátorem právě tehdy, kdy dokáže pomocí mocnin vygenerovat celou zadanou množinu, o čemž jsme se přesvědčili i v příkladech 2.2 a 2.3. Proto tedy platí, že každá grupa, která se skládá z mocnin svého generátoru, je cyklická.

Definice 2.11: Konečná grupa

Grupu nazývané konečnou grupou, pokud je konečná její základní množina. Množinu nazýváme konečnou, jestliže má konečný (spočetný) počet prvků, tedy ji lze vzájemně jednoznačně zobrazit na množinu přirozených čísel.

Definice 2.12: Rozklad grupy

Nechť G je grupa a H její podgrupa, potom systém množin {aH | a ∈ G} nazýváme rozkladem grupy G na levé třídy podle podgrupy H.

Tento rozklad se stručně označuje jako G/H. Množině aH říkáme levá třída grupy G podle podgrupy H.

Definice 2.13: Symetrická grupa

Symetrickou grupou (M, ∘) nazýváme množinu všech permutací na zadané množině spolu s operací skládání funkcí.

Příklad 2.4

Mějme grupu ({A, B}, ∘). U n bodů máme n! permutací, tedy v tomto případě dvě (AB a BA). Můžeme je zapsat v maticích:

$$A = \begin{pmatrix} A & B \\ A & B \end{pmatrix}$$

$$B = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$$

Tabulka s operací skládání funkcí by vypadala následovně:

∘	A	B
A	A	B
B	B	A

Tabulka 3: Operační tabulka skládání funkcí na množině {A, B}

Zjevně je kromě uzavřenosti splněná i komutativita (neboť A ∘ B = B ∘ A), asociativita, existence jednotkového prvku (A) i prvku inverzního (prvky jsou inverzní samy sobě). Jedná se proto o grupu, a v tomto případě i o abelovskou grupu, neboť je i komutativní.

Příklad 2.5

Mějme grupu ({A, B, C}, ∘). Zde máme 3! permutací, tedy šest. V maticovém zápisu budou vypadat následovně:

$$A = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$B = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$C = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

$$D = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

$$E = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$F = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

Jejich tabulka bude se skládáním vypadat takto:

∘	A	B	C	D	E	F
A	A	B	C	D	E	F
B	B	A	E	F	C	D
C	C	D	A	B	F	E
D	D	C	F	E	A	B
E	E	F	B	A	D	C
F	F	E	D	C	B	A

Tabulka 4: Operační tabulka skládání funkcí na množině {A, B, C}

Zde nám na rozdíl od minulého příkladu neplatí komutativita, ale ostatní vlastnosti ano. Jedná se proto o grupu.

Definice 2.14: Permutační grupa

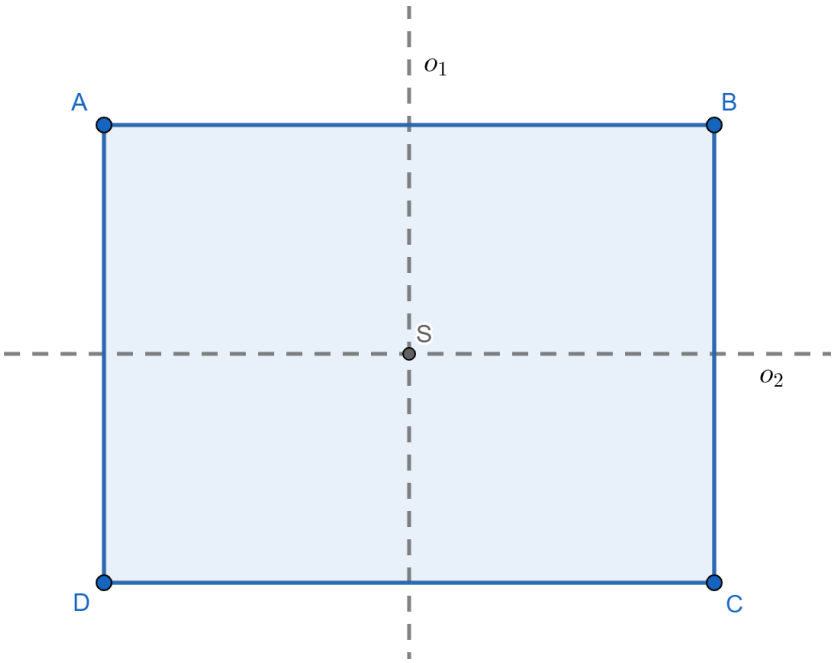
Permutační grupou nazýváme grupu, jejíž prvky jsou permutacemi. Dá se také říct, že se jedná o podmnožinu symetrické grupy.

3 GRUPY SYMETRIÍ GEOMETRICKÝCH OBRAZCŮ

Zajímavým příkladem grup jsou grupy symetrií geometrických obrazců. Mezi symetrie patří nejen osy souměrnosti, ale také rotace. V této kapitole se podíváme na základní obrazce, jimiž jsou rovnostranný trojúhelník, čtverec, obdélník a pravidelný pětiúhelník.

3.1 Obdélník

Zde se nachází čtyři shodná zobrazení. Jedná se o identitu (I), respektive otočení o 0 či 360 stupňů, dále o otočení o 180 °, které zároveň odpovídá i středové souměrnosti (S), a poté o svislou (o_1) a vodorovnou (o_2) osu souměrnosti. Diagonály zde použít nemůžeme, protože máme skutečně obdélník, nikoli čtverec.



Obrázek 2: Symetrie v obdélníku

Maticově tedy můžeme jednotlivá zobrazení a jejich skládání zapsat následně:

Rotace

$$\mathrm{I} = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$$

$$\mathrm{S} = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$$

Osy souměrnosti

$o_1 = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$

$o_2 = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$

Skládání

$S \circ S = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$

$o_1 \circ o_1 = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$

$o_2 \circ o_2 = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$

$S \circ o_1 = o_1 \circ S = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$

$S \circ o_2 = o_2 \circ S = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$

$o_1 \circ o_2 = o_2 \circ o_1 = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$

A nyní již můžeme snadno vytvořit tabulku:

$\circ$	I	S	o_1	o_2
I	I	S	o_1	o_2
S	S	I	o_2	o_1
o_1	o_1	o_2	I	S
o_2	o_2	o_1	S	I

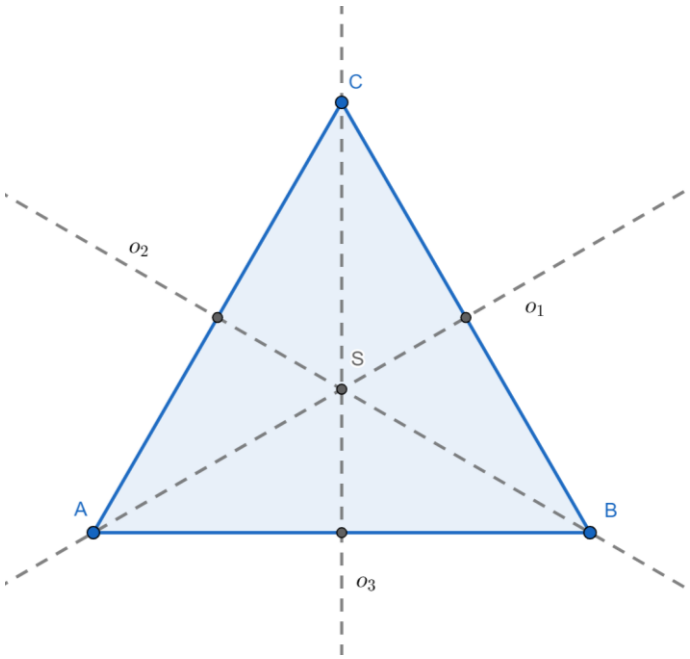
Tabulka 5: Operační tabulka skládání symetrií v obdélníku

Skládání s identitou zachovává neidentickou složku, tedy identita je neutrálním prvkem. Složení dvou stejných os souměrnosti dává identitu.

Výsledkem je proto komutativní (abelovská) grupa, neboť je daná algebraická struktura asociativní i komutativní (symetrická dle diagonály) a kromě neutrálního prvku, jímž je již zmíněná identita, má i prvky inverzní (každé zobrazení je identické samo sobě), protože se v každém řádku i sloupci právě jednou vyskytuje neutrální prvek.

3.2 Rovnostranný trojúhelník

Tento obrazec má celkem 6 shodných zobrazení, a to identitu (I) neboli rotaci o 0 či 360 °, otočení o 120 ° (S), otočení o 240 ° (D) a osy souměrnosti (o_1, o_2, o_3), jimiž jsou spojnice středů stran s protějšími vrcholy.



Obrázek 3: Symetrie v rovnostranném trojúhelníku

Rotace

$$I = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$S = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$D = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

Osy souměrnosti

$$o_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$o_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

$$o_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

∘	I	S	D	o_1	o_2	o_3
I	I	S	D	o_1	o_2	o_3
S	S	D	I	o_2	o_3	o_1
D	D	I	S	o_3	o_1	o_2
o_1	o_1	o_3	o_2	I	D	S
o_2	o_2	o_1	o_3	S	I	D
o_3	o_3	o_2	o_1	D	S	I

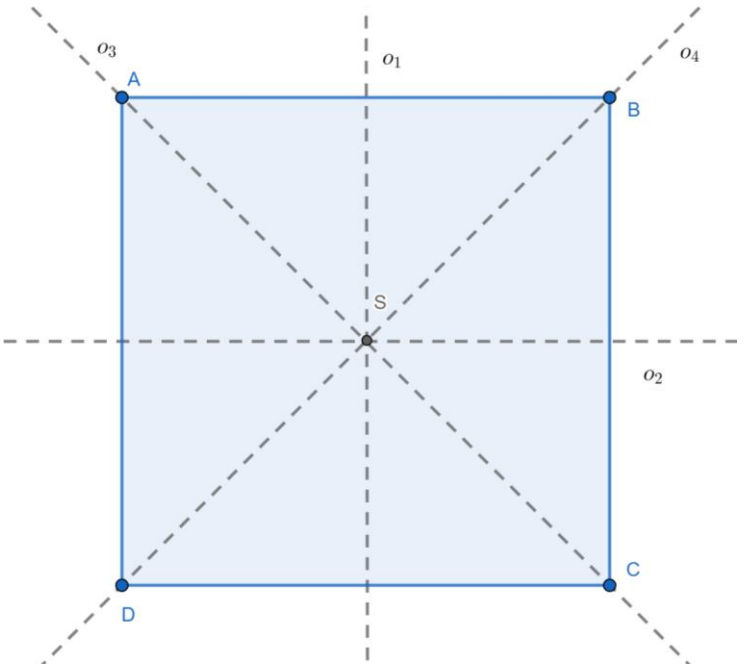
Tabulka 6: Operační tabulka skládání symetrií v rovnostranném trojúhelníku

Skládání s identitou zachovává neidentickou složku, tedy identita je neutrálním prvkem. Složení dvou stejných os souměrnosti dává identitu.

Tato algebraická struktura je grupou, neboť je asociativní, obsahuje neutrální prvek, jímž je již zmíněná identita, a má i prvky inverzní, protože se v každém řádku i sloupci právě jednou vyskytuje neutrální prvek. Komutativita zde neplatí, neboť tabulka není souměrná podle hlavní diagonály. Grupa tedy není komutativní.

3.3 Čtverec

Zde se nachází osm shodných zobrazení, a to čtyři osy – svislá (o_1), vodorovná (o_2) a obě úhlopříčky (o_3 a o_4) – a čtyři rotace – 0 či 360 ° neboli identita (I), 90 ° (P), 180 ° neboli středová souměrnost (S) a 270 ° (D).



Obrázek 4: Symetrie ve čtverci

Rotace

$$I = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}$$

$$P = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$$

$$S = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$$

$$D = \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix}$$

Osy souměrnosti

$$o_1 = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$$

$$o_2 = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$$

$$o_3 = \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}$$

$$o_4 = \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix}$$

∘	I	P	S	D	o_1	o_2	o_3	o_4
I	I	P	S	D	o_1	o_2	o_3	o_4
P	P	S	D	I	o_3	o_4	o_2	o_1
S	S	D	I	P	o_2	o_1	o_4	o_3
D	D	I	P	S	o_4	o_3	o_1	o_2
o_1	o_1	o_4	o_2	o_3	I	S	D	P
o_2	o_2	o_3	o_1	o_4	S	I	P	D
o_3	o_3	o_1	o_4	o_2	P	D	I	S
o_4	o_4	o_2	o_3	o_1	D	P	S	I

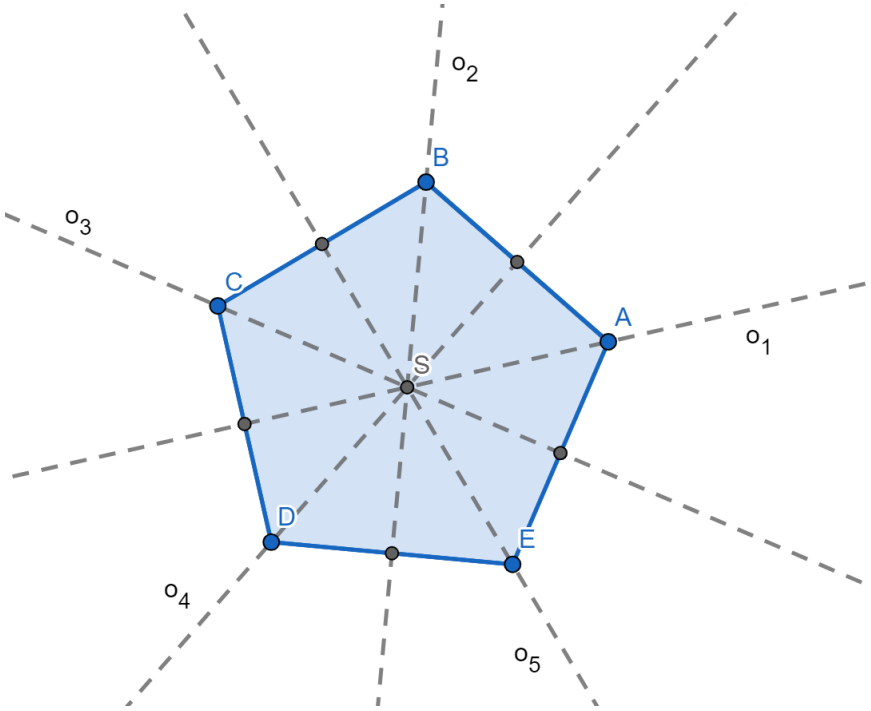
Tabulka 7: Operační tabulka skládání symetrií ve čtverci

Skládání s identitou zachovává neidentickou složku, tedy identita je neutrálním prvkem. Složení dvou stejných os souměrnosti dává identitu.

Tato algebraická struktura je grupou, neboť je asociativní, obsahuje neutrální prvek, jímž je již zmíněná identita, a má i prvky inverzní, protože se v každém řádku i sloupci právě jednou vyskytuje neutrální prvek. Komutativita zde neplatí, neboť tabulka není souměrná podle hlavní diagonály. Grupa tedy není komutativní.

3.4 Pravidelný pětiúhelník

Pravidelný pětiúhelník má 10 symetrií, přesněji řečeno 5 rotací, tedy identitu neboli 0 či 360 ° (I), 72 ° (J), 144°(K), 216 °(L) a 288 °(M) + 5 os souměrnosti (o_1, o_2, o_3, o_4, o_5) což jsou spojnice vrcholů se středy protějších stran.



Obrázek 5: Symetrie v pravidelném pětiúhelníku

Rotace

$$\mathrm{I} = \begin{pmatrix} A & B & C & D & E \\ A & B & C & D & E \end{pmatrix}$$

$$\mathrm{J} = \begin{pmatrix} A & B & C & D & E \\ E & A & B & C & D \end{pmatrix}$$

$$\mathrm{K} = \begin{pmatrix} A & B & C & D & E \\ D & E & A & B & C \end{pmatrix}$$

$$\mathrm{L} = \begin{pmatrix} A & B & C & D & E \\ C & D & E & A & B \end{pmatrix}$$

$$\mathrm{M} = \begin{pmatrix} A & B & C & D & E \\ B & C & D & E & A \end{pmatrix}$$

Osy souměrnosti

$o_1 = \begin{pmatrix} A & B & C & D & E \\ A & E & D & C & B \end{pmatrix}$

$o_2 = \begin{pmatrix} A & B & C & D & E \\ C & B & A & E & D \end{pmatrix}$

$o_3 = \begin{pmatrix} A & B & C & D & E \\ E & D & C & B & A \end{pmatrix}$

$o_4 = \begin{pmatrix} A & B & C & D & E \\ B & A & E & D & C \end{pmatrix}$

$o_5 = \begin{pmatrix} A & B & C & D & E \\ D & C & B & A & E \end{pmatrix}$

∘	I	J	K	L	M	o_1	o_2	o_3	o_4	o_5
I	I	J	K	L	M	o_1	o_2	o_3	o_4	o_5
J	J	K	L	M	I	o_3	o_4	o_5	o_1	o_2
K	K	L	M	I	J	o_5	o_1	o_2	o_3	o_4
L	L	M	I	J	K	o_2	o_3	o_4	o_5	o_1
M	M	I	J	K	L	o_4	o_5	o_1	o_2	o_3
o_1	o_1	o_4	o_2	o_5	o_3	I	K	M	J	L
o_2	o_2	o_5	o_3	o_1	o_4	L	I	K	M	J
o_3	o_3	o_1	o_4	o_2	o_5	J	L	I	K	M
o_4	o_4	o_2	o_5	o_3	o_1	M	J	L	I	K
o_5	o_5	o_3	o_1	o_4	o_2	K	M	J	L	I

Tabulka 8: Operační tabulka skládání symetrií v pravidelném pětiúhelníku

Skládání s identitou zachovává neidentickou složku, tedy identita je neutrálním prvkem. Složení dvou stejných os souměrnosti dává identitu.

Tato algebraická struktura je grupou, neboť je asociativní, obsahuje neutrální prvek, jímž je již zmíněná identita, a má i prvky inverzní, protože se v každém řádku i sloupci právě jednou vyskytuje neutrální prvek. Komutativita zde neplatí, neboť tabulka není souměrná podle hlavní diagonály. Grupa tedy není komutativní.

3.5 Pravidelný n-úhelník

Obecně můžeme říct, že libovolný pravidelný n-úhelník má 2n symetrií, jimiž je:

- n rotací (každý vrchol se může zobrazit sám na sebe i na všechny další vrcholy)
- n os souměrnosti:
    - u lichých n se jedná o osy procházející středem strany a protějším vrcholem
    - u sudých n je n/2 os procházejících středy rovnoběžných stran a n/2 os procházejících dvěma body, které leží naproti sobě

Shodná zobrazení v těchto obrazcích tvoří grupu, neboť skládání je asociativní, obsahuje neutrální prvek (identitu) i prvky inverzní. Obecně ale tato grupa není komutativní.

4 HOMOMORFISMUS A IZOMORFISMUS GRUP

Tato zobrazení mezi dvěma algebraickými strukturami obecně zachovávají nějaké vlastnosti. Homomorfismus zachovává „to důležité“, zatímco izomorfismus je úplně vzájemně jednoznačný, tedy bijektivní, zachovává všechny vlastnosti a každému prvku z jedné množiny přiřazuje právě jeden prvek z množiny druhé.

Definice 4.1: Homomorfismus grup

Grupy (M, *) a (N, $\circ$) jsou homomorfní, pokud u zobrazení f: A → B platí, že:
$\forall a, b \in M$: $f(a * b) = f(a) \circ f(b)$.

Definice 4.2: Izomorfismus grup

Grupy (M, *) a (N, $\circ$) jsou izomorfní, pokud platí, že zobrazení f: A → B je bijekce. Zároveň musí platit také homomorfismus, tedy že:
$\forall a, b \in M$: $f(a * b) = f(a) \circ f(b)$.
Značíme $M \cong N$.

Příklad 4.1

Mějme grupu (M, +), která obsahuje prvky 0, 1, a operaci sčítání modulo 2. Tabulkou je můžeme zapsat takto:

+	0	1
0	0	1
1	1	0

Tabulka 9: Operační tabulka sčítání modulo 2

Dále mějme grupu (N, *), která obsahuje prvky (–1, 1), a operaci násobení. Tabulka by vypadala následovně:

*	1	–1
1	1	–1
–1	–1	1

Tabulka 10: Operační tabulka násobení s prvky (–1, 1)

Na všech místech, kde se v první tabulce vyskytuje nula, se v tabulce druhé vyskytuje jednička. Tam, kde se jednička vyskytuje v první tabulce, máme ve druhé tabulce –1. Můžeme tedy napsat, že $0 \rightarrow 1$ a $1 \rightarrow -1$.

Nyní zbývá ověřit podmínku, že $\forall a, b \in M$: $f(a + b) = f(a) * f(b)$. Máme dva prvky, tedy celkem 4 možnost, jimiž jsou:
$f(0 + 0) = f(0) * f(0)$
Na levé straně $0 + 0 = 0$, což ve druhé tabulce znamená 1.
Na straně pravé pak násobíme nuly, tedy po převedení jedničky a $1 * 1 = 1$.
Rovnost zde platí, neboť $1 = 1$.

$f(0 + 1) = f(0) * f(1)$
$f(1) = 1 * (-1)$
$-1 = -1$

$f(1 + 0) = f(1) * f(0)$
$f(1) = (-1) * 1$
$-1 = -1$

$f(1 + 1) = f(1) * f(1)$
$f(0) = (-1) * (-1)$
$1 = 1$
Na levé straně zde máme v součtu nulu, neboť stále platí, že máme sčítání modulo 2.
Všechny tyto podmínky máme splněny, tedy může říct, že zadané grupy jsou izomorfní.

Věta 4.1

Relace izomorfismu je na množině grup relací ekvivalence.
Relací ekvivalence je relace, která je reflexivní, symetrická a zároveň i tranzitivní.

Věta 4.2: Cayleho věta

Každá grupa je izomorfní s podgrupou permutační grupy.

Definice 4.3: Řád grupy

Řádem konečné grupy (M, *) rozumíme její počet prvků. Značí se |G|.

Definice 4.4: Řád prvku grupy

Mějme grupu (M, *), která má neutrální prvek e. Uvažujme libovolný prvek a ∈ M.

- Existuje-li n ∈ N takové, že $a^n = e$, pak nejmenší takové n nazýváme řádem prvku a.
- Jestliže takové n neexistuje, pak říkáme, že řád prvku je ∞.

Prvek, jehož řád odpovídá řádu grupy, je vždy generátorem.

Věta 4.3: Lagrangeova věta

Mějme konečnou grupu G a její podgrupu H. Poté platí, že $|G| = [G/H] \cdot |H|$, kde |G| je řád grupy G, [G/H] její index podle podgrupy H a |H| je řád podgrupy H.

Index grupy podle podgrupy značí počet tříd. Levé/pravé se zde nerozlišují, neboť je jejich počet, o který v této větě jde, stejný.

Důkaz: Zadaná grupa G je konečná, tedy je konečná i její podgrupa H. Z definice 2.12 víme, že pomocí rozkladu můžeme grupu rozložit na třídy podle podgrupy, tedy že jak levé, tak i pravé třídy obsahují všechny prvky. Vzhledem k tomu, že každá třída má stejný počet prvků (řád), pak toto číslo skutečně musí dělit řád grupy, tedy musí platit, že $|G| = [G/H] \cdot |H|$.

Josef-Louis Lagrange

Tento italský matematik, po němž nese jméno Lagrangeova věta, se narodil roku 1736 v Turínu v severní Itálii. Matematika ho začala zajímat až v 17 letech, kdy náhodou narazil na zajímavou práci matematika Edmonda Halleyho. Již po ročních samostatných studiích z něj byl velmi dobrý matematik. Byl proto jmenován docentem na akademii, kde začal matematiku vyučovat, ale kvůli jeho lhostejné výuce nebyl zrovna ideálním profesorem.

Ve svých 18 letech začal řešit problémy izochronních křivek a přišel na metodu minimalizace a maximalizace funkcionálních zobrazení, která se podobá hledání extrémů funkcí. Vyměnil si také několik dopisů s Leonhardem Eulerem, kterého Lagrangeovy výsledky dosti překvapily, neboť dovedly značně zjednodušit jeho

dřívější rozbory. Díky tomu vznikly Eulerovy-Lagrangeovy rovnice variačního počtu, což jsou soustavy diferenciálních rovnic. I díky nim je Lagrange považován za jednoho ze zakladatelů variačního počtu.

Později byl také jedním ze zakladatelů Turínské akademie věd a kromě matematiky se věnoval i fyzice. Kromě Itálie působil i v Berlíně či Paříži, kde byl také jmenován profesorem a v roce 1813 tam zemřel.

5 KONEČNÉ GRUPY MALÝCH ŘÁDŮ

Grupami malých řádů rozumíme grupy, jejichž řád $n \leq 15$. Pro každé přirozené číslo n existuje minimálně jedna grupa, která má řád n (grupa cyklická). Pro prvočísla zároveň platí, že je cyklická grupa jediná.

Věta 5.1

Grupa s prvočíselným řádem je vždycky cyklická.

Důkaz: Mějme grupu G s prvočíselným řádem n a její libovolný prvek $p \neq 1$. Z Lagrangeovy věty platí, že řád prvku p dělí prvočíslo n, musí tedy být roven n, neboť prvočíslo mimo jedničky jiného dělitele než samo sebe nemá. Z toho plyne, že $G = \langle n \rangle$.

Věta 5.2

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

Důkaz: Mějme grupu prvočíselného řádu G a její nejednotkovou podgrupu H s libovolným nejednotkovým prvkem h. Podle věty 5.1 platí, že $G = \{h\} \leq H$, tedy $G = H$, grupa G nemá vlastní podgrupy.

Jestliže g je libovolný nejednotkový prvek grupy G, potom $\{g\} = G$ a grupa G je cyklická. Jelikož nekonečná cyklická grupa má nekonečně mnoho vlastních podgrup, potom musí být grupa G konečnou cyklickou grupou. Pokud by její řád byl složeným číslem, musela by obsahovat nějakou vlastní podgrupu. Grupa G proto musí být cyklickou grupou prvočíselného řádu.

5.1 Grupy prvočíselných řádů

Z předchozí věty víme, že grupy, jejichž řádem je prvočíslo (u malých řádů 2, 3, 5, 7, 11 a 13), musí být cyklické. Snadno tedy sestrojíme jejich operační tabulky. Názorným příkladem mohou být třeba grupy na množině Z s operací sčítání modulo n.

+	0	1
0	0	1
1	1	0

Tabulka 11: Operační tabulka se sčítáním modulo 2

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabulka 12: Operační tabulka se sčítáním modulo 3

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabulka 13: Operační tabulka se sčítáním modulo 5

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tabulka 14: Operační tabulka se sčítáním modulo 7

+	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

Tabulka 15: Operační tabulka se sčítáním modulo 11

+	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12	0
2	2	3	4	5	6	7	8	9	10	11	12	0	1
3	3	4	5	6	7	8	9	10	11	12	0	1	2
4	4	5	6	7	8	9	10	11	12	0	1	2	3
5	5	6	7	8	9	10	11	12	0	1	2	3	4
6	6	7	8	9	10	11	12	0	1	2	3	4	5
7	7	8	9	10	11	12	0	1	2	3	4	5	6
8	8	9	10	11	12	0	1	2	3	4	5	6	7
9	9	10	11	12	0	1	2	3	4	5	6	7	8
10	10	11	12	0	1	2	3	4	5	6	7	8	9
11	11	12	0	1	2	3	4	5	6	7	8	9	10
12	12	0	1	2	3	4	5	6	7	8	9	10	11

Tabulka 16: Operační tabulka se sčítáním modulo 13

Definice 5.1: Normální podgrupa

Podgrupu H nazýváme normální (nebo také invariantní) podgrupou grupy G, pokud platí, že:

$\forall h \in h, \forall g \in G: g \cdot h \cdot g^{-1} \in H$

Grupa, která nemá žádné normální podgrupy, se nazývá jednoduchá.

Definice 5.2: Faktorová grupa

Mějme grupu G a její normální podgrupu H. Množina levých tříd grupy G podle podgrupy H společně s binární operací $aH \cdot bH = (a \cdot b)H$ tvoří opět grupu, které říkáme faktorová grupa či zkráceně faktor-grupa. Značíme ji G/H.

Lemma 5.1

Mějme grupu G, v níž pro každý prvek a platí, že $a^2 = 1$. Potom G je Abelova grupa.

Důkaz: Mějme libovolné prvky a, b z grupy G a vztah $1 = (ab)^2 = abab$. Pokud ho zleva vynásobíme prvkem ba, pak dostaneme $ba = baabab$. Vzhledem k tomu, že $a^2 = b^2 = 1$, je rovnost $ab = ba$ dokázána.

Grupy řádu 4

Tyto grupy můžeme rozdělit na dvě části:

1) V grupě G existuje prvek řádu 4. Jde tedy o cyklickou grupu, u níž snadno sestrojíme operační tabulku:

	1	a	a^2	a^3
1	a	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 17: Cyklická grupa řádu 4

2) Prvek řádu 4 zde neexistuje, ale z důsledku Lagrangeovy věty plyne, že mají všechny nejednotkové prvky řád 2, tedy podle lemmatu 5.1 musí být grupa komutativní.

Dva různé nejednotkové prvky označíme a, b. Víme, že $a^2 = b^2 = 1$ a že $ab = ba$. Nyní již není problém napsat operační tabulku:

	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 18: Kleinova čtyřgrupa (necyklická grupa řádu 4)

Grupy řádu 6

I tyto grupy si nejprve rozdělíme na dvě části:

1) V grupě G existuje prvek řádu 6. Jde tedy o cyklickou grupu, u níž snadno sestrojíme 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 19: Cyklická grupa řádu 6

2) Prvek řádu 6 zde neexistuje. Z Lagrangeovy věty plyne, že nejednotkové prvky musejí být řádu 2 nebo 3. Kdybychom měli pouze prvky řádu 2, musela by tato grupa obsahovat Kleinovu čtyřgrupu, což dle Lagrangeovy věty možné není (čtyřka nedělí šestku).

   Musí tedy existovat prvek a, který není 1, ale platí u něj, že $a^3 = 1$. Kromě prvků 1, a, b ($= a^2$) tedy potřebujeme ještě c, d ($= ac$) a e ($= a^2c = bc$). Nyní máme všech šest prvků, které pro sestrojení grupy potřebujeme.

   Ještě potřebujeme ukázat, že $c^2 = 1$. Jelikož v grupě platí zákon krácení zprava i zleva, rychle nás možnosti jako $c^2 = c$, $c^2 = ac$ či $c^2 = a^2c$ dovedou ke sporu s tím, že prvek c je různý od 1, a, b. Pokud by neplatilo, že $c^2 = 1$, pak by prvek c měl řád tři, tedy $c^3 = 1$, což dává spor stejně jako možnost $a^2 = c^2$. Rovnost $c^2 = 1$ tedy platit musí.

Stejným způsobem se můžeme přesvědčit, že i $d^2 = e^2 = 1$. První možnosti nám vyřadí zákon krácení zprava i zleva a další řády.

	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 20: Necyklická grupa řádu 6

U této struktury je jasně vidět, že není komutativní. Zbývá ještě ověřit, zda vůbec je grupou. Z tabulky můžeme snadno vidět, že má neutrální prvek, jímž je jednička, má prvky inverzní, protože se jednička vyskytuje právě jednou v každém řádku i sloupci. Ověřit asociativnost by bylo značně složité, nicméně dle [1] zde platí, že $\varphi(1) = \mathrm{Id}$, $\varphi(a) = (123)$, $\varphi(b) = (132)$, $\varphi(c) = (12)$, $\varphi(d) = (23)$ a $\varphi(e) = (13)$, což je izomorfismus na symetrickou grupu 3. stupně.

Každá grupa řádu 6 je tedy izomorfní s cyklickou grupou Z_6 nebo se symetrickou grupou stupně 3.

Již zde můžeme vidět, že čím vyšší řád máme, tím je nalézání grup komplikovanější. Nyní proto přistoupíme k dalším definicím a větám, které nám studium grup vyšších řádů usnadní, neboť v nich budeme moct využívat grupy řádů nižších.

Definice 5.3: Vnější direktní součin

Mějme grupy H, K; $h \in H$, $k \in K$. Jejich vnějším direktním součinem rozumíme množinu všech uspořádaných dvojic (h, k) spolu s binární operací $(h_1, k_1) \cdot (h_2, k_2) = (h_1h_2, k_1k_2)$, která je opět grupou. Značíme $G = H \times K$.

Definice 5.4: Vnitřní direktní součin

Mějme dvě normální podgrupy grupy G, které označíme H, K. Jestliže $H \cup K = G$ a $H \cap K = 1$. Pak G je vnitřním direktním součinem grup H, K. Značíme $G = H \times K$.

Lemma 5.2

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

Mezi vnitřním a vnějším direktním součinem však není nutné rozlišovat. Mějme dvě grupy H, K a jejich vnější direktní součin $G = H \times K$. Označme $H' = \{(h, 1), h \in H\}$ zobrazení $\varphi(h) = (h, 1)$, které je izomorfismem H na H′. Totéž platí i u K, kde $K' = \{(1, k), k \in K\}$ je zobrazení $\varphi(k) = (1, k)$, což je izomorfismus K na K′.

Nyní vezměme rovnost $(h, 1) \cdot (1, k) = (h, k) = (1, k) \cdot (h, 1)$. Ta nám ukazuje, že G je vnitřním direktním součinem grup H′ a K′, což jsou grupy izomorfní s grupami H a K. Totéž můžeme použít i obráceně, tedy mít vnitřní direktní součin grup H, K a vnější direktní součin grup H′, K′, které jsou opět vzájemně izomorfní.

Věta 5.3

Direktní součin dvou cyklických grup s nesoudělnými řády m, n je opět cyklickou grupou řádu mn.

Důkaz: Mějme cyklickou grupu $H = \{a\}$ řádu m a cyklickou grupu $K = \{b\}$ řádu n. Pak jejich direktní součin $G = H \times K$ obsahuje prvky ve tvaru $a^r b^s$, přičemž $0 \leq r < m$ a $0 \leq s < n$, z čehož plyne, že $o(G) \leq mn$.

Platí, že $(ab)^{mn} = a^{mn} \cdot b^{mn} = 1$. Kdyby pro nějaké t platilo, že $(ab)^t = 1$, pak $1 = (ab)^{mt} = a^{mt} \cdot b^{mt} = b^{mt}$. Z toho plyne, že $n|mt$ a z ohledem na $(n, m) = 1$ také $n|t$. Analogicky také $m|t$, tedy $[m, n]|t$. Věta však hovoří o nesoudělných grupách, tedy násobek $[m, n] = mn$ neboli řád prvku ab je v grupě G součin mn a můžeme napsat, že $G = \{ab\}$.

Definice 5.5: Periodická grupa

Abelova grupa, která nemá prvky nekonečného řádu, se nazývá periodická či torzní.

Věta 5.4

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

Definice 5.6: P-grupa

Každá konečná grupa řádu p^n, kde p značí prvočíslo a $n \in N$, se nazývá p-grupou.

Věta 5.5

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

Věta 5.6

G je Abelova grupa a p^k její prvek maximálního řádu (což znamená, že pro všechna $g \in G$ platí, že $o(g) \leq p^k$). Cyklická grupa {a} je pak direktním činitelem v G, tedy $G = \{a\} \times H$.

Věta 5.7

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

Důkaz: Grupa G řádu p je z věty 5.1 grupou cyklickou. Mějme tedy grupu řádu p^n, kde $n > 1$. Dále předpokládejme, že je každá abelovská p-grupa řádu menšího než p^n direktním součinem cyklických grup.

Jestliže je prvek $a \in G$ prvkem maximálního řádu v G, pak dle věty 5.6 platí, že $G = \{a\} \times H$. H je však dle předpokladu direktní součin cyklických grup.

Věta 5.8

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

U každé konečné Abelovy grupy G nám věty 5.5 a 5.7 zajišťují existenci direktního rozkladu. Grupa G pak jednoznačně určuje řády cyklických direktních činitelů. Tyto řády nazýváme invarianty grupy G. Dvě konečné Abelovy grupy jsou izomorfní právě tehdy, když mají soustavy těchto invariantů stejné. Ke každé soustavě invariantů pak existuje konečná komutativní grupa, jejíž soustava invariantů se rovná soustavě invariantů předem zadané.

V tuto chvíli se již dostáváme k obecnému postupu, který nám pomůže nalézt všechny komutativní grupy řádu n:

1) Jestliže je $n = p_1^{k1} \cdot p_2^{k2} \cdot \ldots \cdot p_r^{kr}$ zápis čísla n v kanonickém tvaru, pak je grupa G dle věty 5.5 direktním součinem svých p_i-primárních komponent G_{pi}, kde $i = 1, 2, \ldots, r$. Řády těchto komponent G_{pi} jsou pak zřejmě p_i, kde $i = 1, 2, \ldots, r$.
2) Věta 5.7 nám říká, že je každá grupa G_{pi} direktním součinem cyklických grup řádů $p_i^{ki1}, p_i^{ki2}, \ldots, p_i^{kis}$, přičemž $k_{i1} + k_{i2} + \ldots + k_{isi} = k_i$ pro $i = 1, 2, \ldots, r$, $s_i \in N$. Potřebujeme tedy nalézt všechna vyjádření daného čísla k_i ve tvaru součtu několika sčítanců z N, abychom mohli nalézt všechny možné direktní rozklady komponenty G_{pi}.
3) K případnému zjednodušení direktního rozkladu můžeme ještě využít větu 5.3.

5.2 Komutativní grupy neprvočíselných řádů

Konečné komutativní grupy řádu 4

a) $2^1, 2^1$

b) $G = Z_2 \times Z_2$ (Kleinova čtyřgrupa)

c) 2^2

$G = Z_4$ (cyklická grupa řádu 4)

Obě jejich operační tabulky jsou již sestrojené výše.

Konečné komutativní grupy řádu 6

a) $2^1, 3^1$

$Z_2 \times Z_3$, což můžeme zjednodušit na Z_6 (cyklická grupa řádu 6)

Operační tabulka této grupy je již sestrojená výše.

Konečné komutativní grupy řádu 8

a) 2^3

$G = Z_8$ (cyklická grupa řádu 8)

b) $2^2, 2^1$

$G = Z_4 \times Z_2$

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

$G = Z_2 \times Z_2 \times Z_2$

	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 21: Cyklická grupa řádu 8

Pro grupu Z_4 x Z_2 zvolme pro první cyklickou grupu jako generátor prvek a, u něhož musí platit, že $a^4 = 1$. Pro druhou grupu pak b, kde $b^2 = 1$. Zároveň zde také platí, 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 22: Grupa Z_4 x Z_2

Pro grupu Z_2 x Z_2 x Z_2 již budeme potřebovat tři prvky a, b, c, u nichž platí, že $a^2 = b^2 = c^2 = 1$. Opět zde platí, že 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	b
bc	bc	abc	c	b	ac	ab	1	a
abc	abc	bc	ac	ab	c	b	a	1

Tabulka 23: Grupa Z_2 x Z_2 x Z_2

Konečné komutativní grupy řádu 9

a) 3^2

G = Z_9 (cyklická grupa řádu 9)

b) 3^1, 3^1

G = Z_3 x Z_3

	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 24: Cyklická grupa řádu 9

Pro grupu Z_3 x Z_3 potřebujeme dva generátory a, b, u nichž musí platit, že $a^3 = b^3 = 1$. I zde také platí, 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 25: Grupa Z_3 x Z_3

Konečné komutativní grupy řádu 10

a) 5^1, 2^1

G = Z_5 x Z_2, což můžeme zjednodušit na Z_{10} (cyklická grupa řádu 10)

	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 26: Cyklická grupa řádu 10

Konečné komutativní grupy řádu 12

a) $2^2, 3^1$

$G = Z_4 \times Z_3$, což můžeme zjednodušit na Z_{12} (cyklická grupa řádu 12)

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

$G = Z_2 \times Z_2 \times Z_3$, což můžeme zjednodušit na $Z_2 \times Z_6$

	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 27: Cyklická grupa řádu 12

Pro grupu Z_2 x Z_6 budeme mít generátor a, pro nějž musí platit, že $a^2 = 1$, a b, pro který $b^6 = 1$. Opět zde také platí, 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	b^2	ab^4	ab^5	a	ab	ab^2
b^4	b^4	ab^4	b^5	1	b	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 28: Grupa Z_2 x Z_6

Konečné komutativní grupy řádu 14

a) $2^1, 7^1$

$G = Z_2 \times Z_4$, což můžeme zjednodušit na Z_{14} (cyklická grupa řádu 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}
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 29: Cyklická grupa řádu 14

Konečné komutativní grupy řádu 15

a) $3^1, 5^1$

$G = Z_3 \times Z_5$, což můžeme zjednodušit na Z_{15} (cyklická grupa řádu 15)

	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 30: Cyklická grupa řádu 15

Prozatím jsme na řadě příkladů zjišťovali, že až na izomorfismus lze klasifikaci konečných komutativních grup poměrně snadno provést. Celý postup popsal německý matematik Leopold Kronecker (1823–1891). Tento postup se stal jakousi ukázkou ideální algebraické teorie.

Příklad 5.1

Popište až na izomorfismus všechny komutativní grupy, které mají 100 prvků.

Můžeme říct, že $100 = 2^2 \cdot 5^2$. Platí, že každá komutativní grupa je direktním součinem svých p-primárních komponent. Pro prvočíslo $p = 2$ máme dvě možnosti: Z_{2^2}, tedy Z_4, a $Z_2 \oplus Z_2$. Pro $p = 5$ máme také dvě možnost: Z_{25} a $Z_5 \oplus Z_5$.

Kombinací těchto možností získáme následující:

a) $Z_4 \oplus Z_{25} \cong Z_{100}$ (neboť čísla 4 a 25 jsou nesoudělná)
b) $Z_4 \oplus Z_5 \oplus Z_5 \cong Z_{20} \oplus Z_5$
c) $Z_2 \oplus Z_2 \oplus Z_{25} \cong Z_2 \oplus Z_{50}$
d) $Z_2 \oplus Z_2 \oplus Z_5 \oplus Z_5 \cong Z_{10} \oplus Z_{10}$

5.3 Nekomutativní grupy neprvočíselných řádů

Nyní jsme se věnovali komutativním grupám, u nichž platilo, že buďto byly cyklické, nebo se daly získat s pomocí dvou či tří generátorů. Existují ale i grupy nekomutativní, na které se zaměříme nyní. Grupám řádu 4 a 6 jsme se již obecně věnovali na začátku kapitoly, proto nyní budeme pokračovat od řádu 8.

Konečné nekomutativní grupy řádu 8

Budeme-li mít osmiprvkovou nekomutativní grupu G, pak víme, že nemůže mít prvek řádu 8, neboť by v takovém případě byly cyklická (takže komutativní). Z lemmatu 5.1 plyne také to, že nemůže obsahovat samé prvky řádu 2. Musí proto obsahovat prvek řádu 4, který označíme a.

Grupa $A = \{a\}$ je cyklickou grupou řádu 4, u níž $[G : A] = 2$. Platí také tvrzení, že pokud H je podgrupa grupy G, u níž platí, že $[G : H] = 2$, tak $H \Delta G$. Takže $A \Delta G$ a faktorová grupa G/A má řád 2. Mějme prvek $b \in G$ takový, že $b \notin A$. Pak $(bA)^2 = b^2A = A$, takže $b^2 \in A$.

V úvahu nyní připadají možnosti $b^2 = 1$, $b^2 = a$, $b^2 = a^2$ a $b^2 = a^3$. Pokud by platilo, že $b^2 = a$, byla by $\{b\}$ cyklickou grupou (takže komutativní), stejně by tomu bylo i v případě $b^2 = a^3$, i zde bychom dostali cyklickou grupu. Zůstávají nám tedy možnosti, že $b^2 = 1$ a $b^2 = a^2$.

Víme, že je grupa A normální podgrupou grupy G, tudíž můžeme napsat, že $b^{-1}ab = a^n$ pro $n = 0, 1, 2, 3$. Možnost $b^{-1}ab = a^0$ můžeme rovnou vyloučit, neboť bychom se dostavili do sporu, že $ab = b$. U varianty $b^{-1}ab = a^1$ bychom získali $ab = ba$, což je také spor, neboť to značí komutativitu. Z $b^{-1}ab = a^2$ dostaneme, že $b^{-1}a^2b = b^{-1}ab \cdot b^{-1}ab =$ $= a^2 \cdot a^2 = 1$, tedy $a^2b = b$, takže $a^2 = 1$, což je spor. Nyní zůstává pouze možnost $b^{-1}ab = a^3$.

Mohou tedy existovat dvě nekomutativní grupy s řádem 8, které můžeme definovat takto:

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

Pro sestrojení tabulky potřebujeme zapsat ba^n jako a^xb^y. Máme $b^{-1} = b$, $bab = a^3$, $ba = a^3b$. Tudíž $ba^2 = ba \cdot a = a^3ba = a^3 \cdot a^3b = a^2b$ a $ba^3 = ab$. Nyní již můžeme napsat tabulku:

	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 31: Nekomutativní grupa řádu 8 s relacemi $a^4 = 1, b^2 = 1, b^{-1}ab = a^3$

Ve druhém případě budeme potřebovat rovnosti $ba = a^3b$, $ba^2 = a^2b$, $ba^3 = ab$. Prvky máme stejné jako v případě prvním. Operační tabulka tedy budeme vypadat následovně:

	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 32: Nekomutativní grupa řádu 8 s relacemi $a^4 = 1, b^2 = a^2, b^{-1}ab = a^3$ (grupa kvaternionů)

Získali jsme skutečně dvě nekomutativní grupy řádu 8, neboť ani jedna z tabulek není souměrná podle hlavní diagonály.

Nyní nás čekají nekomutativní grupy devátého řádu, pro které však budeme potřebovat jednu důležitou podgrupu a dvě nové věty.

Definice 5.7: Centrum grupy

Mějme grupu G. Potom množinu $Z = \{z \in G;\ zg = gz \text{ pro všechna } g \in Z\}$ nazýváme jejím centrem.

Věta 5.9

Centrum Z libovolné grupy G je komutativní podgrupou dané grupy. Každá podgrupa centra grupy G je zároveň normální podgrupou grupy G.

Věta 5.10

Každá konečná p-grupa má netriviální centrum. To znamená, že prvočíslo p dělí řád centra Z.

Konečné nekomutativní grupy řádu 9

Je zřejmé, že grupy řádu 9 budou 3-grupy. Centra této grupy mohou s ohledem na větu 5.10 být tří- či devítiprvková. Ovšem v případě devíti prvků by grupa nutně musela být komutativní. Zbývá nám tedy pouze možnost tříprvkového centra, tedy $b^3 = 1$ a $Z = \{b\}$.

Musí také existovat prvek $a \in G$, který však nenáleží Z. Stejně tak $a^2 \notin Z$, což znamená, že prvek a je řádu 3. $\{a\} \cap \{b\} = 1$ a $b \in Z$, tedy $ab = ba$. Odtud se však již dostáváme k tomu, že všechny prvky můžeme napsat jako součin $a^r b^s$, kde $0 \leq r \leq 2$, totéž pro s. Vzhledem k tomu, že prvek a pak komutuje s každým prvkem součinu, pak jistě $A \in Z$, čímž se dostáváme ke sporu.

Z tohoto tedy plyne, že žádná nekomutativní grupa řádu 9 neexistuje.

Nyní nám zbývá prostudovat nekomutativní grupy řádu 10, 12, 14 a 15. Nejprve se zaměříme na ty z nich, jejichž řád jde rozložit na součin dvou navzájem různých

prvočísel p, q. Budou to grupy řádů 10, 14 a 15. Využijeme u nich ještě některé nové definice a věty.

Definice 5.8: Sylowovská p-grupa

Mějme grupu G s řádem $p^n \cdot m$, kde $(m, p) = 1$. Každou podgrupy této grupy řádu p^n nazýváme sylowovskou p-grupou grupy G.

Definice 5.9: Konjungovaný prvek

Mějme grupu G a její prvky g, h. Prvek h je konjungován s prvkem g v G, pokud existuje prvek $x \in G$ takový, že $h = x^{-1}gx$. Stejně tak podgrupy H, K grupy G jsou konjungovány v G právě tehdy, když existuje prvek $x \in G$ takový, že platí $x^{-1}Hx = K$.

Věta 5.11

Mějme konečnou grupu G řádu n a prvočíslo p, které řád grupy dělí. Grupa G potom obsahuje sylowovskou p-podgrupu.

Sylowovy věty

Jedná se o trojici vět (někdy se toto číslo liší, ale obsah zůstává stejný), které částečně souvisejí s větou Lagrangeovou. Jméno nesou podle norského matematika Petera Ludwiga Mejdella Sylowa (1832–1918).

Věta 5.12: 1. Sylowova věta

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

Věta 5.13: 2. Sylowova věta

Každé dvě sylowovské p-podgrupy konečné grupy G jsou konjungované.

Věta 5.14: 3. Sylowova věta,

Mějme konečnou grupu G a prvočíslo p, které dělí řád zadané grupy. Potom počet všech sylowovských p-podgrup grupy G dělí o(G) a je roven $1 + kp$, kde k je jisté nezáporné celé číslo.

Konečné nekomutativní grupy řádu 10

Dle věty 5.14 bude grupa řádu 10 obsahovat sylowovské 5-podgrupy, jichž bude $1 + 5k$, kde $k = 0, 1, 2, \ldots$ Vzhledem k tomu, že $1 + 5k$ musí dělit 10, je jedinou možností $k = 0$. To by v G existovala jediná sylowovská 5-podgrupa A, která by byla normální podgrupou grupy G a zároveň cyklickou pětiprvkovou grupou s generátorem a, tedy $A = \{a\}$, $a^5 = 1$, $A \Delta G$.

Dále bude grupa řádu 10 obsahovat sylowovské 2-podgrupy, kterých bude $1 + 2r$. To platí pro $r = 0$, $r = 2$. Pro $r = 0$ bychom měli jedinou sylowovskou 2-podgrupu B, kde $b^2 = 1$, $B \Delta G$. Dvě normální podgrupy grupy G {a}, {b}, které jsou cyklické a mají nesoudělné řády, můžeme podle věty 5.3 zjednodušit na cyklickou grupu řádu 10, která jistě není komutativní.

Nyní nám ale zbývá ještě $r = 2$. Po dosazení do vzorečku $1 + 2r$ dostáváme číslo 5, tedy má grupa G celkem 5 sylowovských 2-podgrup. Označme jednu z nich {b}, $b^2 = 1$. Protože $A \Delta G$, bude $b^{-1}ab \in A$, tedy $b^{-1}ab = a^n$, $n = 1, 2, 3, 4, 5$. Následně $a = b^{-2}ab^2 = = b^{-1} \cdot b^{-1}ab \cdot b = b^{-1}a^nb = b^{-1}ab \cdot b^{-1}ab \cdot \ldots b^{-1}ab = a^{n^2}$. Prvek $b^{-1}ab$ je v součinu n-krát.

Jelikož je prvek a řádu 5, potom n^2 dá při dělení tímto řádem vždy zbytek 1. Díky tomu nám zbude akorát $n = 1$ a $n = 4$. Pokud by platilo, že $b^{-1}ab = a^4$, získali bychom $ab = ba$, tedy komutativní grupu. Zbývá proto jedině $n = 4$. Pro tuto možnost máme relace $a^5 = 1$, $b^2 = 1$ a $b^{-1}ab = a^4$, jejímž převedením získáme $ab = ba^4$.

Nyní zbývá převést ba^3, ba^2 a ba. Prvek $ba^3 = ba^3 \cdot a^5 = ba^4 \cdot a^4 = aba^4 = a^2b$. Stejným způsobem $ba^2 = a^3b$ a $ba = a^4b$. Můžeme již sestrojit i operační tabulku:

	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 33: Nekomutativní grupa řádu 10 (Cayleyho tabulka)

Existují tedy dvě grupy řádu 10. První z nich je cyklická grupa, a tedy komutativní, druhá nekomutativní.

Nekomutativní grupy řádu 14

Grupa řádu 14 bude obsahovat jedinou sylowovskou 7-podgrupu, což bude normální podgrupa grupy G, označíme ji {a} s tím, že $a^7 = 1$.

Dále zde zjevně budeme mít i sylowovské 2-podgrupy. Aby platilo, že $1 + 2m$ dělí 14, můžeme mít buďto $m = 0$ nebo $m = 3$. S jedinou sylowovskou podgrupou {b} rovnou dostaneme, že G = {a} x {b}, což by byla cyklická grupa řádu 14.

Nyní nám tedy zbývá $m = 3$, pro které existuje 7 sylowovských 2-podgrup. Jednou z nich je {b}, $b^2 = 1$, což není normální podgrupa, ale {a} již ano. Z toho plyne, že $b^{-1}ab = a^r$, r je zde jisté přirozené číslo menší než 8. Nyní již můžeme vyvodit, že $a^1 = a^{r^2}$, tedy $r^2 \equiv 1 \bmod 7$. Odtud nám vyjde, že $r = 1$ či $r = 6$. Ovšem pro $r = 1$ bychom dostali komutativní grupu, proto $r = 6$.

Máme tedy relace $a^7 = 1$, $b^2 = 1$, $b^{-1}ab = a^6$. Po převedení pak dostane i $ba = ba \cdot a^7 = ba^6 \cdot a^2 = aba^2 = a \cdot a^5b = a^6b$ a obdobně $ba^2 = a^5b$, $ba^3 = a^4b$, $ba^3 = a^4b$, $ba^4 = a^3b$, $ba^5 = a^2b$, $ba^6 = ab$. S těmito relacemi již můžeme snadno sestrojit operační tabulku:

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

Tabulka 34: Nekomutativní grupa řádu 14

I u řádu 14 tedy máme celkem dvě grupy, které nejsou izomorfní. Jedná se o cyklickou grupu a grupu nekomutativní.

Nekomutativní grupy řádu 15

V grupě řádu 15 určitě musí být sylowovská 5-podgrupa, která zjevně bude jediná (pro číslo 0), a tedy i normální. Dále musíme mít sylowovskou 3-podgrupu, ovšem i ta bude jediná i normální. S ohledem na větu 5.3 tedy můžeme říct, že žádná nekomutativní grupa řádu 15 neexistuje.

Řád 15 má tedy jediná grupa, a to grupa cyklická.

Nekomutativní grupy řádu 12

Vraťme se nyní ke grupám řádu 12, které jsme vynechali, neboť číslo 12 není součinem dvou různých prvočísel. Máme zde však zvláštní případ, a to p^2q, kde opět platí, že p, q jsou navzájem různá prvočísla.

Jistě musí grupa řádu 12 obsahovat sylowovské 3-podgrupy. Aby vztah $1 + 3r$ dělil číslo 12, můžeme mít $r = 0$ nebo $r = 1$. Tato sylowovská podgrupa tedy buďto bude jediná, konkrétně normální (v případě $r = 0$), nebo budou 4 navzájem konjungované (pro $r = 1$).

Dále bude grupa řádu 12 určitě obsahovat i 2-podgrupy řádu 4, u nichž podmínky $1 + 2s$ a dělitel 12 splňuje opět $s = 0$ a $s = 1$. I nyní můžeme říct, že tato sylowovská podgrupa buďto bude jediná a normální, nebo budou 3 navzájem konjungované.

V tuto chvíli mohou teoreticky nastat 4 případy:

1) Bude existovat jediná sylowovská 2-podgrupa řádu 4, kterou označíme A, a zároveň jediná sylowovská 3-podgrupa B. S ohledem na to, že $G \Delta A$ a $G \Delta B$, můžeme říct, že $G = A \times B$ a G tedy je komutativní grupou, která již byla uvedena.
2) Možnost, při níž by hledaná grupa G obsahovala 4 sylowovské 3-podgrupy a ještě 3 vzájemně konjugované sylowovské 2-podgrupy, nastat zjevně nemůže, neboť máme řád pouze 12, tedy 12 prvků, zatímco tato možnost by jich vyžadovala 18.
3) Bude existovat jediná sylowovská 3-podgrupa $A = \{a\}$ a 3 navzájem konjugované sylowovské 2-podgrupy. Jednu z nich označíme B.

a. Předpokládejme, že B je cyklická grupa řádu 4, v níž $B = \{b\}$ a $b^4 = 1$. Jelikož A je normální podgrupou grupy G, můžeme říct, že $b^{-1}ab = a^r$, kde $r = 0, 1, 2$. První dvě možnosti ihned vyloučíme, neboť s nulou získáme $ab = b$ a $a = 1$, což je spor, a jednička vede na rovnost $ab = ba$, což by znamenalo komutativní grupu.

   Jediná zbývající možnost je $r = 2$, tedy $b^{-1}ab = a^2$. Kromě této rovnosti, z níž přenásobením prvkem b zleva ihned získáme $ba^2 = ab$, máme definující relace $a^3 = 1$ a $b^4 = 1$, díky čemuž již může převést zápisy na tvar a^xb^y.

   $ba = ba \cdot a^3 = ba^2 \cdot a^2 = ab \cdot a^2 = aab = a^2b$ a obdobně $b^2a = ab^2$, $b^3a = = a^2b^3$, $b^2a^2 = a^2b^2$ a $b^3a^2 = ab^3$. V tuto chvíli již můžeme sestrojit 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	1	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^3	a	b^2	b^3	1	a^2b^2	a^2b^3	a^2
ab^2	ab^2	a^2b^2	b^2	ab^3	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 35: Nekomutativní grupa řádu 12 s relacemi $a^3 = 1$, $b^4 = 1$ a $b^{-1}ab = a^2$

b. Tentokrát budeme předpokládat, že B je Kleinova čtyřgrupa (pro b, c, kde $b^2 = c^2 = 1$ a $bc = cb$). Víme, že A je normální podgrupou grupy G a $b^{-1}ab = a^r$. Pro nulu bychom dostali spor, že $a = 1$, zbývá tedy $r = 1, 2$. Podobně u $c^{-1}ac = a^s$ můžeme mít $s = 1, 2$. Pro dvojici čísel mohou nastat čtyři případy:

i. $r = s = 1$, což by ale vedlo na komutativní grupu

ii. $r = 1$, $s = 2$, zde ale můžeme přeznačit r, s na b, c. Tím bychom dostali relace $a^3 = 1$, $b^2 = c^2 = 1$, $bc = cb$, $b^{-1}ab = a$ $(ab = ba)$, $c^{-1}ac = a^2$ $(ac = ca^2)$. Tyto relace skutečně určují další nekomutativní grupu řádu 12.

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

$ca = ca \cdot a^3 = ca^2 \cdot a^2 = ac \cdot a^2 = a \cdot ca^2 = a \cdot ac = a^2c$

Nyní sestrojíme operační tabulku:

	1	a	a^2	b	c	ab	ac	bc	abc	a^2b	a^2c	a^2bc
1	1	a	a^2	b	c	ab	ac	bc	abc	a^2b	a^2c	a^2bc
a	a	a^2	1	ab	ac	a^2b	a^2c	abc	a^2bc	b	c	bc
a^2	a^2	1	a	a^2b	a^2c	b	c	a^2bc	bc	ab	ac	abc
b	b	ab	a^2b	1	bc	a	abc	c	ac	a^2	a^2bc	a^2c
c	c	a^2c	ac	bc	1	a^2bc	a^2	b	a^2b	abc	a	ab
ab	ab	a^2b	b	a	abc	a^2	a^2bc	ac	a^2c	1	bc	c
ac	ac	c	a^2c	abc	a	bc	1	ab	b	a^2bc	a^2	a^2b
bc	bc	a^2bc	abc	c	b	a^2c	a^2b	1	a^2	ac	ab	a
abc	abc	bc	a^2bc	ac	ab	c	b	a	1	a^2c	a^2b	a^2
a^2b	a^2b	b	ab	a^2	ac	1	bc	a^2c	c	a	abc	ac
a^2c	a^2c	ac	c	a^2bc	a^2	abc	a	a^2b	ab	bc	1	b
a^2bc	a^2bc	abc	bc	a^2c	a^2b	ac	ab	a^2	a	c	b	1

Tabulka 36: Nekomutativní grupa řádu 12 s relacemi $a^3 = 1$, $b^2 = c^2 = 1$, $bc = cb$, $ab = ba$, $ac = ca^2$

iii. $r = 2$, $s = 1$, tento případ je stejný jako případ ii., pouze s opačným přeznačením prvků.

iv. $r = s = 2$, zde by muselo platit $b^{-1}ab = a^2$, $c^{-1}ac = a^2$. Můžeme ale přeznačit prvky b, c na bc, c, čímž se opět dostaneme k předchozím dvěma bodům.

4) V grupě G bude existovat jediná sylowovská 2-podgrupa A řádu 4 a celkem 4 vzájemně konjungované sylowovské 3-podgrupy. Rozdělíme si zde 2 možnosti:

a. Grupa A bude cyklickou grupou řádu 4, v níž $a^4 = 1$. Grupa B bude jednou ze sylowovských 3-podgrup, v níž $b^3 = 1$. Platí, že A Δ G, tedy $b^{-1}ab = a^r$ pro r = 0, 1, 2, 3. Nula nám dá ihned spor, že b = ab, číslo 1 nás dovede ke komutativní grupě, v níž ab = ba. Zbývají nám možnosti r = 2, 3, ovšem nutné kongruenci $r^3 \equiv 1 \mod 4$ nevyhovuje ani jedna z nich.
b. Nyní místo cyklické grupy řádu 4 uvažujme Kleinovu čtyřgrupu, v níž $a^2 = b^2 = 1$, ab = ba a grupa A je normální podgrupou grupy G. Grupa G pak bude jednou z konjugovaných sylowovských 3-podgrup, kde B = {c} a $c^3 = 1$. Nyní musí platit, že $c^{-1}ac = a^k b^l$, $c^{-1}bc = a^m b^n$, přičemž každé z čísel k, l, m, n je buďto 0, nebo 1. Rovnou ale můžeme vyloučit k = l = 0 i m = n = 0, neboť by $a^k b^l$ i $a^m b^n$ muselo být rovno jedné, a to je spor. Zbývá nám tedy celkem 9 možností:
    i. k = l = 1, m = n = 1, tedy $c^{-1}ac = ab$, $c^{-1}bc = ab$, což nastat určitě nemůže, protože z rovnosti $c^{-1}ac = c^{-1}bc$ plyne, že a = b, a to je spor.
    ii. k = l = 1, m = 1, n = 0, tedy $c^{-1}ac = ab$, $c^{-1}bc = a$. Tento případ nastat může.
    iii. k = l = 1, m = 0, n = 1 neboli $c^{-1}ac = ab$, $c^{-1}bc = b$. Zde dostaneme spor, že a = ab.
    iv. k = 1, l = 0, m = n = 1 neboli $c^{-1}ac = a$, $c^{-1}bc = ab$. Ani tato možnost nenastane, protože zde vyjde, že b = ab.
    v. k = 1, l = 0, m = 1, n = 0, tedy $c^{-1}ac = a$, $c^{-1}bc = a$. Z těchto rovností plyne, že $c^{-1}ac = c^{-1}bc$ neboli a = b, což je určitě spor.
    vi. k = 1, l = 0, m = 0, n = 1, tedy $c^{-1}ac = a$, $c^{-1}bc = b$. Zde můžeme rovnou vidět, že ac = ca, bc = cb, což by byla komutativní grupa.
    vii. k = 0, l = 1, m = n = 1 neboli $c^{-1}ac = b$, $c^{-1}bc = ab$. Nyní dostáváme totéž, co ve druhé možnosti, pouze s přeznačenými prvky.
    viii. k = 0, l = 1, m = 1, n = 0 neboli $c^{-1}ac = b$, $c^{-1}bc = a$. Tady máme opět spor, že a = b.

ix. $k = 0, l = 1, m = 0, n = 1$, tedy $c^{-1}ac = b$, $c^{-1}bc = b$. Opět vychází, že $c^{-1}ac = c^{-1}bc$, tedy $a = c$, což je určitě spor.

Z bodů 2 a 7 můžeme vidět, že existuje i třetí nekomutativní grupa řádu 12. Její relace jsou $a^2 = b^2 = 1$, $ab = ba$, $c^3 = 1$, $c^{-1}ac = ab$ ($abc = cb$), $c^{-1}bc = a$ ($bc = ca$). Můžeme nyní sestrojit její operační tabulku:

	1	a	b	c	c^2	ab	ac	ac^2	bc	bc^2	abc	abc^2
1	1	a	b	c	c^2	ab	ac	ac^2	bc	bc^2	abc	abc^2
a	a	1	ab	ac	ac^2	b	c	c^2	abc	abc^2	bc	bc^2
b	b	ab	1	bc	bc^2	a	abc	abc^2	c	c^2	ac	ac^2
c	c	bc	abc	c^2	1	ac	bc^2	b	abc^2	ab	ac^2	a
c^2	c^2	abc^2	ac^2	1	c	bc^2	ab	abc	a	ac	b	bc
ab	ab	b	a	abc	abc^2	1	bc	bc^2	ac	ac^2	c	c^2
ac	ac	abc	bc	ac^2	a	c	abc^2	ab	bc^2	b	c^2	1
ac^2	ac^2	bc^2	c^2	a	ac	abc^2	b	bc	1	c	ab	abc
bc	bc	c	ac	bc^2	b	abc	c^2	1	ac^2	a	abc^2	ab
bc^2	bc^2	ac^2	abc^2	b	bc	c^2	a	ac	ab	abc	1	c
abc	abc	ac	c	abc^2	ab	bc	ac^2	a	c^2	1	bc^2	b
abc^2	abc^2	c^2	bc^2	ab	abc	ac^2	1	c	b	bc	a	ac

Tabulka 37: Nekomutativní grupa řádu 12 s relacemi $a^2 = b^2 = 1$, $ab = ba$, $c^3 = 1$, $c^{-1}ac = ab$, $c^{-1}bc = a$

Nyní můžeme konstatovat, že grup řádu 12 máme hned 5, dvě z nich jsou komutativní a další tři nekomutativní.

Závěrem ještě konstatujme, že s popisem nekomutativních grup mohou být spojeny velké potíže. Takovou zkušenost získali i nejlepší světoví matematici, když se pokusili popsat všechny konečné jednoduché nekomutativní grupy. Kromě očekávaných tříd grup ale nalezli i tzv. sporadické grupy. Těch je celkem 26 a největší z nich má přibližně $8 \cdot 10^{53}$ prvků.

ZÁVĚR

Tato práce nejprve shrnovala základy v podobě binárních operací a algebraických struktur, které jsou pro zkoumání grup nezbytné. Ve druhé kapitole se již zaměřila na konkrétní struktury, mezi které patří nejen grupy, ale i třeba pologrupy či monoidy. Bylo zde uvedeno i několik příkladů, které slouží ke snadnějšímu porozumění.

Třetí kapitola se věnovala velmi zajímavé skupině grup, přesněji řečeno grupám symetrií geometrických obrazců. Postupně se v ní objevily základní obrazce, jimiž jsou čtverec, obdélník, rovnostranný trojúhelník a pravidelný pětiúhelník. U každého z nich se nachází přehled veškerých symetrií, tedy rotací a os souměrnosti, ale i operační tabulky s jejich skládáním. Na závěr je zde obecné shrnutí těchto zobrazení v pravidelných n-úhelnících.

Ve čtvrté kapitole se mohou čtenáři seznámit s pojmy homomorfismus a izomorfismus grup. Kromě definic a podrobného příkladu se zde nachází i několik vět, včetně věty Lagrangeovy, která je jednou ze základních vět z teorie grup.

Poslední pátá kapitola se již věnuje klíčovému tématu této práce – konečným grupám malých řádů. Přináší ještě několik důležitých vět a definic, ale především se věnuje samotným grupám. Nejprve jsou to intuitivní grupy prvočíselných řádů, následně nejmenších neprvočíselných řádů, a nakonec i složitější grupy, které se ještě dělí na komutativní a nekomutativní. U veškerých řádů najde čtenář vypsané všechny grupy i sestrojené jejich operační tabulky. Stejně tak se zde nacházejí i postupy, jak takové grupy lze najít.

RESUMÉ

Tato bakalářská práce se věnuje teorii grup, konkrétně konečným grupách malých řádů. První kapitola obsahuje základy v podobě binárních operací, po nichž ve druhé kapitole následují základní algebraické struktury, mezi které patří i grupy. Kapitola třetí hovoří o grupách symetrií základních geometrických obrazců. Čtvrtá kapitola pak seznamuje s pojmy homomorfismus a izomorfismus grup.

Poslední a zároveň nejrozsáhlejší je pátá kapitola, která se věnuje hlavnímu tématu, tedy konečným grupám malých řádů, což znamená řád nanejvýš 15. Kromě postupů, jak je najít, zde čtenář najde i sestrojené operační tabulky.

RESUME

This bachelor's thesis is devoted to group theory, specifically to finite groups of small orders. The first chapter contains the basics like binary operations, followed by basic algebraic structures, including groups, in the second chapter. The third chapter talks about groups of symmetries of basic geometric shapes. The fourth chapter introduces the concepts of homomorphism and isomorphism of groups.

The last and at the same time the most extensive chapter is the fifth chapter, which deals with the main topic, i.e. finite groups of small orders, which means order at most 15. In addition to the procedures for finding them, the reader will also find here the constructed operational tables.

SEZNAM LITERATURY

[1] Hora, J.: Konečné grupy malých řádů, sborník PF v Plzni Matematika V, 1989 (strany 56–73)

[2] Beran, L.: Grupy a svazy, Praha, SNTL, 1974

[3] Honzík, L.: Pomocný text k předmětu Elementární algebra [online]. Plzeň, 2021. Dostupné z: courseware předmětu KMT/ELA

[4] Gollová, A.: Konečné grupy [online]. Praha. Dostupné z: https://math.fel.cvut.cz/en/people/gollova/mkr/mkr5.pdf

[5] Čechová, I.: Konečné grupy malých řádů [online]. Plzeň, 2012. Dostupné z: https://dspace5.zcu.cz/handle/11025/5433. Bakalářská práce. Západočeská univerzita v Plzni. Vedoucí práce: doc. RNDr. Jaroslav Hora, CSc.

[6] Kuřil, M.: Základy teorie grup [online]. Ústí nad Labem. Dostupné z: https://kma.ujep.cz/administrace/uploads/afa9832.pdf

[7] Suchánek, V.: Permutační grupy [online]. Brno, 2018. Dostupné z: https://is.muni.cz/th/g8hn2/suchanek.pdf. Bakalářská práce. Masarykova univerzita. Vedoucí práce: prof. RNDr. Radan Kučera, DSc.

[8] Évariste Galois. In: Wikipedia: The Free Encyclopedia [online]. Dostupné z: https://en.wikipedia.org/wiki/%C3%89variste_Galois

[9] Niels Henrik Abel. In: Wikipedia: The Free Encyclopedia [online]. Dostupné z: https://en.wikipedia.org/wiki/Niels_Henrik_Abel

[10] Abelian variety. In: Wikipedia: The Free Encyclopedia [online]. Dostupné z: https://en.wikipedia.org/wiki/Abelian_variety

[11] Abel Prize. In: Wikipedia: The Free Encyclopedia [online]. Dostupné z: https://en.wikipedia.org/wiki/Abel_Prize

[12] Joseph Louise Lagrange. In: Wikipedia: The Free Encyclopedia [online]. Dostupné z: https://en.wikipedia.org/wiki/Joseph-Louis_Lagrange

[13] Sporadic group. In: Wikipeda: The Free Encyclopedia [online]. Dostupné z: https://en.wikipedia.org/wiki/Sporadic_group

[14] Isibalo. 10 – Grupa symetrií obdélníku (MAT – Abstraktní algebra). YouTube, 2019. Dostupné z: https://youtu.be/C1pDjS1ZMs0

[15] Isibalo. 17 – Izomorfismus grupoidů (MAT – Abstraktní algebra). YouTube, 2019. Dostupné z: https://youtu.be/mv3rv4gpnVI

[16] Isibalo. 18 – Hledání izomorfismu grupoidů (MAT – Abstraktní algebra). YouTube, 2019. Dostupné z: https://youtu.be/zrpm-Ri4ZZY

[17] Isibalo. 23 – Cyklická grupa (MAT – Abstraktní algebra). YouTube, 2020. Dostupné z: https://youtu.be/sHqIUJw3bWY

[18] Isibalo. 31 – Lagrangeova věta (MAT – Abstraktní algebra). YouTube, 2021. Dostupné z: https://youtu.be/sEbaUJgcaLI

[19] Isibalo. 33 – Normální (invariantní) podgrupa (MAT – Abstraktní algebra). YouTube, 2021. Dostupné z: https://youtu.be/Gh-OZL3gbT8

[20] By Johan Gørbitz - Originally uploaded to English wikipedia by en:User:Pladask, http://www.math.uio.no/div/abelkonkurransen/, Public Domain, https://commons.wikimedia.org/w/index.php?curid=90392

SEZNAM OBRÁZKŮ, TABULEK, GRAFŮ A DIAGRAMŮ

Tabulka 1: Operační tabulka násobení na množině Z_5 6

Tabulka 2: Přehled vlastností jednotlivých algebraických struktur 9

Tabulka 3: Operační tabulka skládání funkcí na množině {A, B} 14

Tabulka 4: Operační tabulka skládání funkcí na množině {A, B, C} 15

Tabulka 5: Operační tabulka skládání symetrií v obdélníku 17

Tabulka 6: Operační tabulka skládání symetrií v rovnostranném trojúhelníku 19

Tabulka 7: Operační tabulka skládání symetrií ve čtverci 20

Tabulka 8: Operační tabulka skládání symetrií v pravidelném pětiúhelníku 22

Tabulka 9: Operační tabulka sčítání modulo 2 24

Tabulka 10: Operační tabulka násobení s prvky (–1, 1) 24

Tabulka 11: Operační tabulka se sčítáním modulo 2 28

Tabulka 12: Operační tabulka se sčítáním modulo 3 29

Tabulka 13: Operační tabulka se sčítáním modulo 5 29

Tabulka 14: Operační tabulka se sčítáním modulo 7 29

Tabulka 15: Operační tabulka se sčítáním modulo 11 30

Tabulka 16: Operační tabulka se sčítáním modulo 13 30

Tabulka 17: Cyklická grupa řádu 4 31

Tabulka 18: Kleinova čtyřgrupa (necyklická grupa řádu 4) 32

Tabulka 19: Cyklická grupa řádu 6 32

Tabulka 20: Necyklická grupa řádu 6 33

Tabulka 21: Cyklická grupa řádu 8 37

Tabulka 22: Grupa $Z_4 \times Z_2$ 37

Tabulka 23: Grupa $Z_2 \times Z_2 \times Z_2$ 38

Tabulka 24: Cyklická grupa řádu 9 38

Tabulka 25: Grupa Z_3 x Z_3 39

Tabulka 26: Cyklická grupa řádu 10 39

Tabulka 27: Cyklická grupa řádu 12 40

Tabulka 28: Grupa Z_2 x Z_6 41

Tabulka 29: Cyklická grupa řádu 14 42

Tabulka 30: Cyklická grupa řádu 15 43

Tabulka 31: Nekomutativní grupa řádu 8 s relacemi $a^4 = 1$, $b^2 = 1$, $b^{-1}ab = a^3$ 45

Tabulka 32: Nekomutativní grupa řádu 8 s relacemi $a^4 = 1$, $b^2 = a^2$, $b^{-1}ab = a^3$ (grupa kvaternionů) 45

Tabulka 33: Nekomutativní grupa řádu 10 (Cayleyho tabulka) 48

Tabulka 34: Nekomutativní grupa řádu 14 49

Tabulka 35: Nekomutativní grupa řádu 12 s relacemi $a^3 = 1$, $b^4 = 1$, $b^{-1}ab = a^2$ 51

Tabulka 36: Nekomutativní grupa řádu 12 s relacemi $a^3 = 1$, $b^2 = c^2 = 1$, $bc = cb$, $ab = ba$, $ac = ca^2$ 52

Tabulka 37: Nekomutativní grupa řádu 12 s relacemi $a^2 = b^2 = 1$, $ab = ba$, $c^3 = 1$, $c^{-1}ac = ab$, $c^{-1}bc = a$ 54

Obrázek 1: Niels Henrik Abel 10

Obrázek 2: Symetrie v obdélníku 16

Obrázek 3: Symetrické v rovnostranném trojúhelníku 18

Obrázek 4: Symetrie ve čtverci 19

Obrázek 5: Symetrie v pravidelném pětiúhelníku 21