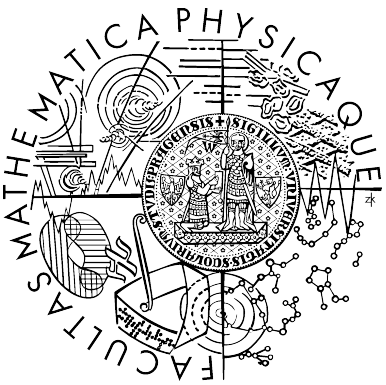
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Jiří Sláma

Grupy malých řádů

Katedra didaktiky matematiky
Vedoucí diplomové práce: *Doc. RNDr. Jindřich Bečvář, CSc.*
Studijní program: *Matematika, učitelství matematiky*
pro střední školy v kombinaci s informatikou

Rád bych poděkoval panu doc. RNDr. Jindřichu Bečvářovi, CSc., za odborné vedení mé práce, za rady a za čas, který mi během vypracovávání této práce věnoval.

Prohlašuji, že jsem svou diplomovou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce.

V Praze dne 9. 4. 2008 Jiří Sláma

Obsah

Název práce: *Grupy malých řádů*
Autor: *Jiří Sláma*
Katedra (ústav): *Katedra didaktiky matematiky*
Vedoucí diplomové práce: *Doc. RNDr. Jindřich Bečvář, CSc.*
E-mail vedoucího: *becvar@karlin.mff.cuni.cz*
Abstrakt:
Po úvodním výkladu obsahujícím základní pojmy a výsledky teorie grup následuje partie o Sylowových podgrupách, mj. formulace a důkazy tří Sylowových vět, které jsou základním nástrojem k popisu struktury zejména nekomutativních grup.
Další výklad je směřován k popisu všech konečných grup až do řádu 15 včetně. V zásadě existují dva odlišné přístupy k charakterizaci těchto grup – na jedné straně se lze zaměřit právě na tyto konkrétní grupy, na straně druhé lze popsat grupy, jejichž řád je např. mocninou prvočísla, a získané výsledky použít v daném případě. Tato práce se snaží o rozumný kompromis mezi oběma přístupy, tj. o jakousi zlatou střední cestu mezi přílišnou specifičností a komplikovaností. V důsledku toho pojednání zahrnuje i popis všech konečných Abelových grup. Výklad je prostoupen demonstrativními příklady, přičemž je kladen důraz na nalezení příkladů grup i z oblasti mimo čistou matematiku.

Klíčová slova: *teorie grup, konečné grupy, Sylowovy věty, Abelovy grupy*.

Title: *Groups of Small Orders*
Author: *Jiří Sláma*
Department: *Department of Mathematics Education*
Supervisor: *Doc. RNDr. Jindřich Bečvář, CSc.*
Supervisor's e-mail address: *becvar@karlin.mff.cuni.cz*
Abstract:
The first part of the thesis presents elementary facts and results of the theory of groups. The second part explains Sylow's subgroups theory containing, among others, formulations and proofs of the three Sylow's theorems which are important tools in analysing the structure of mainly nonabelian groups.
The goal of the following part is to describe the structure of all finite groups up to order 15. Basically, there are two possible approaches to the characterization of these groups – one can either focus just on these particular groups or describe groups with order of e.g. prime power and then use the results to solve the task.
The author of this thesis chooses reasonable middle ground between overly specific approach and one too complicated. As a result of this choice, the description of all finite abelian groups is included. The theory is illustrated with some demonstrative examples, with emphasis on those outside of „the pure matematics“.

Keywords: *theory of groups, finite groups, Sylow's theorems, Abelian groups.*

„Básníci jsou tu od toho, aby dávali jedné věci mnoho jmen.
U matematiků je tomu naopak.“

(anonym)

Úvod

Hlavním cílem této práce je popsat strukturu všech konečných grup do řádu 15 včetně.

Záměrně byl zvolen styl výkladu, který se poněkud odklání od tradičního matematického postupu definice, věta, důkaz. Domnívám se, že tento zvolený způsob poskytuje větší prostor pro uvedení souvislostí, nadto reflektuje autorem studovaný obor – učitelství matematiky.

Práce je rozdělena do osmi hlavních kapitol, které se dále dělí na části.

První kapitola obsahuje základní pojmy a výsledky teorie grup, které jsou potřeba pro porozumění dalším pasážím. Po úvodním přehledu elementárních pojmů následuje definice nekomutativní i komutativní grupy spolu s jejich příklady, dále vysvětlení grupového homomorfismu, resp. izomorfismu. Na definici grupy navazuje popis podgrupy, a to včetně tzv. *alternativního kritéria pro podgrupy*. Výklad je opět doprovázen příklady. Při hlubším zkoumání podgrup dospíváme ke třídám grupy podle podgrupy, Lagrangeově větě a následně i k normálním podgrupám a faktorizaci podle normálních podgrup. Práce obsahuje též osvětlení problematiky konjugovaných podgrup, následované prvním dílčím výsledkem analýzy struktury grup malých řádů – popisem cyklických grup. V závěru první kapitoly jsou popsány základní vlastnosti homomorfismu a je také definován direktní součin grup.

Následující kapitola popisuje strukturu všech konečných komutativních grup – nejprve je zaveden pojem p-primární komponenta, následně ukážeme, že každou komutativní grupu lze vyjádřit jako direktní součin jistých p-primárních komponent. Opět je kladen důraz na grupy řádu maximálně 15.

Třetí kapitola zobecňuje pojem p-primární komponenty, zavedený ve druhé kapitole, a zavádí Sylowovy podgrupy.

Kapitola čtvrtá obsahuje formulace a důkazy tří Sylowových vět, které jsou základním nástrojem k popisu struktury zejména nekomutativních grup. První Sylowova věta je jakousi obrácenou verzí Lagrangeovy věty – garantuje existenci podgrup jistých řádů. Druhá Sylowova věta ukazuje, že všechny Sylowovy p-podgrupy dané grupy jsou izomorfní. Konečně třetí Sylowova věta vypovídá o počtu Sylowových p-podgrup.

Pátá kapitola se zabývá klasifikací doposud neprobraných grup řádu maximálně 15. Nejprve jsou probrány grupy řádu p^2, resp. pq, resp. $2p$. Po nich přichází na řadu charakteristika zbývajících řádů, konkrétně řádů 8 a 12.

Následující kapitola je jakýmsi atlasem všech grup až do řádu 15 včetně. Uvedena je celá řada informací. Předně je to název grupy, doplněný popisem a zpravidla i příklady. Dále u většiny grup nalezneme hned tři různé způsoby popisu vnitřní struktury. Nejznámějším je zřejmě popis formou tzv. *Cayleyho tabulek*, z nich lze snadno vyčíst, jak je definována grupová operace. Kromě těchto tabulek zde nalezneme i grafy cyklů, které graficky znázorňují cyklické podgrupy dané grupy a jejich vzájemné vztahy. Poslední informací o grupách jsou Hasseovy diagramy, ty zachycují veškeré podgrupy dané grupy a jejich vzájemnou inkluzi, značením navazují na Cayleyho tabulky. Hlavním rozdílem mezi Hasseovými diagramy a grafy cyklů je „volba základních elementů“ – zatímco u Hasseových diagramů je základním elementem podgrupa, u grafu cyklů je to prvek grupy.

V předposlední kapitole jsou informativně zmíněny grupy řádů 16 až 20, čtenář je přitom upozorněn na grupy, jejichž konstrukce je analogická konstrukci některé z grup menšího řádu.

Kapitola je uzavřena přehlednou tabulkou s počty komutativních a nekomutativních grup jednotlivých řádů.

Poslední kapitola uvádí příklady oblastí, ve kterých se čtenář může setkat s konceptem grupy. Stručně jsou zmíněny grupy geometrických transformací (včetně zmínky o tzv. *Erlangenském programu*), grupa cest v bludišti, Galoisova grupa permutací kořenů polynomu. Následuje užití grup při řešení hlavolamů, zmíněna je Rubikova kostka a „patnáctka“. Posledním tématem jsou krystalografické grupy spolu s jednoduššími analogiemi – Friezovými grupami a tzv. *wallpaper* grupami.

Základy teorie grup

1 Elementární pojmy

Množinou rozumíme souhrn objektů, kterým říkáme prvky. Každý prvek se v množině může vyskytovat nejvýše jednou. Náleží-li prvek a množině M, zapisujeme tento fakt $a \in M$, v opačném případě užijeme zápisu $a \notin M$. Množina neobsahující žádný prvek se nazývá prázdná množina, značíme ji $\emptyset$. Je-li každý prvek množiny M současně i prvkem množiny N, řekneme, že množina M je podmnožinou množiny N, značíme $M \subseteq N$. Prázdná množina je zřejmě podmnožinou každé množiny. Množina je zřejmě podmnožinou sebe sama, hovoříme o nevlastní podmnožině. Je-li $M \subseteq N$ a zároveň $N \subseteq M$, mluvíme o rovnosti množin a píšeme $M = N$. Průnikem množin M, N rozumíme množinu prvků, které se vyskytují současně v obou množinách, píšeme $M \cap N$. Je-li průnikem dvou množin prázdná množina, hovoříme o nich jako o množinách disjunktních. Sjednocením množin M, N je množina, obsahující prvky, které se vyskytují alespoň v jedné z daných množin, označujeme

$$M \cup N .$$

Rozkladem množiny rozumíme třídu vesměs disjunktních množin, jejichž sjednocením je původní množina.

Kartézským součinem množin M, N nazveme množinu

$$M \times N = \{(m, n); m \in M, n \in N\} .$$

Relací (binární relací) na množině M rozumíme podmnožinu kartézského součinu $M \times M$. Relaci R na množině M nazveme

reflexivní, pokud

$$\forall a \in M : (a, a) \in R ,$$

symetrickou, pokud

$$\forall a, b \in M : (a, b) \in R \rightarrow (b, a) \in R ,$$

tranzitivní, jestliže

$$\forall a, b, c \in R : (a, b) \in R \wedge (b, c) \in R \rightarrow (a, c) \in R ,$$

konečně antisymetrickou, když

$$\forall a, b \in R : (a, b) \in R \wedge (b, a) \in R \rightarrow a = b .$$

Relace, která je reflexivní, symetrická a tranzitivní se nazývá ekvivalence.

Relace ekvivalence nám může posloužit k definování rozkladu dané množiny M – pokud utvoříme třídu jejích podmnožin tak, že do stejné podmnožiny zařadíme prvky, které jsou v ekvivalenci, získáme rozklad množiny M.

Z reflexivity je zřejmé, že každý prvek se musí v nějaké množině rozkladu vyskytovat, tedy po sjednocení musíme získat celou původní množinu M. Ukažme, že třídy rozkladu jsou navzájem disjunktní, jinak řečeno – mají-li dvě množiny

$$M_a = \{x \in M ; (x, a) \in R\} , \; M_b = \{x \in M ; (x, b) \in R\}$$

neprázdný průnik, jsou totožné. Vskutku, je-li

$$x \in M_a \cap M_b ,$$

je $(a, b) \in R$. Je-li $y \in M_a$, je $y \in M_b$. Dokázali jsme tedy inkluzi

$$M_a \subseteq M_b .$$

Analogicky se dokáže i inkluze opačná, dohromady můžeme vyvodit, že $M_a = M_b$.

Binární operací na neprázdné množině *M* rozumíme zobrazení

$$f : M \times M \to M ,$$

které každé uspořádané dvojici $(a, b) \in M$ přiřazuje právě jeden prvek $c \in M$. Tento fakt zapisujeme ve tvaru $f(a, b) = c$, případně $afb = c$.

Množiny přirozených, celých, racionálních a reálných čísel označujeme po řadě

$$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R} .$$

2 Grupa

V této kapitole uvedeme definici grupy. Tento pojem patří k základům algebry, jedná se o přirozené zobecnění struktur, které potkáváme kolem sebe, a to nejen v mnoha odvětvích matematiky (geometrie, analýza, algebra), ale i tam, kde bychom to vůbec nečekali, např. v hudbě či při skládání Rubikovy kostky.

Grupou rozumíme množinu *G* spolu s definovanou binární operací „·“, která má tyto vlastnosti:

1. $\forall a, b, c \in G: (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asociativita)
2. $\exists e \in G \ \forall a \in G: a \cdot e = e \cdot a = a$ (existence neutrálního prvku)
3. $\forall a \in G \ \exists b \in G: a \cdot b = b \cdot a = e$ (existence inverzních prvků).

Předchozí tři požadavky nazýváme *axiomy grupy*.

Poznámka: Samozřejmě se můžeme setkat i s jiným značením dané operace, nejčastěji se ovšem užívá tento tzv. *multiplikativní zápis*, my zde navíc nadále budeme používat i tradiční zkrácený multiplikativní zápis, tj. zcela bez označení operace.

První axiom říká, že nezáleží na uzávorkování, ale pouze na pořadí činitelů, druhý zaručuje existenci tzv. *neutrálního prvku*, tj. prvku, kterým lze vynásobit libovolný prvek grupy beze změny výsledku. Konečně, třetí axiom tvrdí, že pro každý prvek existuje takový prvek (tzv. *prvek inverzní*), že po jejich vzájemném vynásobení vyjde prvek neutrální, zmiňovaný v axiomu č. 2.

Poznámka: Abychom byli přesní, musíme připustit, že tento systém pravidel nesplňuje jeden z požadavků mnohdy na axiomy kladených – totiž požadavek minimálnosti množiny požadavků. Dá se ukázat, že místo druhého a třetího požadavku stačí trvat na existenci levého neutrálního a levých inverzních prvků, tj. na systému axiomů

1'. $\forall a, b, c \in G: (a \cdot b) \cdot c = a \cdot (b \cdot c)$

2'. $\exists e \in G \ \forall a \in G: e \cdot a = a$

3'. $\forall a \in G \ \exists b \in G: b \cdot a = e$.

Existenci pravého jednotkového prvku a pravých inverzních prvků lze dokázat z této množiny axiomů.

Z původních axiomů sice vyplývá existence neutrálního prvku, ovšem ne jeho jednoznačnost. Tu lze ovšem snadno dokázat – nechť e, e' jsou dva neutrální prvky, pak $ee' = e'$, neboť e je neutrální, zároveň však i $ee' = e$, neboť e' je neutrální, tedy $e = ee' = e'$.

Stejně snadno lze ukázat, že ke každému prvku existuje maximálně jeden inverzní prvek (spolu s 3. axiomem tedy získáváme, že ke každému prvku existuje právě jeden inverzní prvek) – nechť b, c jsou dva inverzní prvky k prvku a, tedy platí $ba = ab = e$ a zároveň $ca = ac = e$. Pak zřejmě

$$b = be = b(ac) = (ba)c = ec = c,$$

tedy $b = c$ (plyne z definice jednotkového prvku a asociativity grupové operace). Prvek inverzní k prvku a budeme nadále značit a^{-1}.

Grupou tedy rozumíme neprázdnou množinu spolu s binární operací na ní definovanou, přičemž požadujeme asociativitu této operace, existenci (právě jednoho) neutrálního prvku a dále ke každému prvku existenci (právě jednoho) prvku inverzního.

Pokud kromě výše zmíněných axiomů platí navíc

$$\forall a, b \in G: ab = ba \text{ (komutativita)},$$

hovoříme o *komutativní*, též *Abelově* grupě. Komutativní grupy většinou uvažujeme jako aditivní, grupovou operaci tedy označujeme jako „+“, hovoříme o neutrálním prvku a o opačných prvcích.

Je-li $n \in \mathbb{N}$ počet prvků grupy G, řekneme, že G je konečná a číslo n prohlásíme jejím řádem, v opačném případě řekneme, že G je nekonečná. V této práci se budeme zabývat zejména grupami do řádu 15 včetně, tedy grupami majícími maximálně 15 prvků. Pokusíme se nalézt všechny existující grupy až do tohoto řádu. Je zřejmé, že grupu lze zadat tak, že všechny prvky množiny označíme symboly a poté definujeme binární operaci (říkejme jí nadále násobení), která bude odpovídat daným axiomům. Snadno nahlédneme, že nezáleží na tom, jak prvky označíme, zda 1, 2, 3, α, β, γ či A, B, C – důležité je, jakým způsobem definujeme onu operaci.

Jednou z možností, jak to provést, je použít tzv. *Cayleyho tabulku*, která bude v záhlaví obsahovat symboly odpovídající jednotlivým prvkům a uvnitř odpovídající součiny. Tedy budeme-li hledat nějakou grupu o třech prvcích, stačí do následující tabulky doplnit součiny odpovídajících prvků (e značí jednotkový prvek):

	e	a	b
e	?	?	?
a	?	?	?
b	?	?	?

Tabulka 1: Cayleyho tabulka, před vyplněním

Na první pohled bychom mohli očekávat až 3^9 (19 683) možností, jak tabulku vyplnit. Ale již pohled na druhý axiom (existence neutrálního prvku) nám ukáže, že v prvním řádku, resp. sloupci, se musí záhlaví opakovat:

	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

Tabulka 2: Cayleyho tabulka, násobení jednotkovým prvkem

Poznámka: Samozřejmě lze za jednotkový prvek zvolit kterýkoliv ze zbývajících dvou, nicméně potom stačí v nové tabulce přeznačit a přesunout sloupce a řádky a dostaneme tabulku stávající.

Nyní se nám počet možností zmenšil na 3^4 (81). K dalšímu zúžení počtu možností můžeme s úspěchem užít větu, která nám říká, že grupová operace je tzv. *operace s krácením*, tj.

$$\forall a, b, c \in G: (ab = ac \rightarrow b = c) \wedge (ba = ca \rightarrow b = c).$$

Dokažme pouze první část (viz [3], str. 20): nechť $ab = bc$, pak

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c,$$

druhá část se dokáže analogicky (využívá se existence inverzního prvku a asociativity).

Podívejme se nyní, co nám tato věta poskytuje při doplňování tabulky. Pokud bychom chtěli např. do prvního řádku s otazníky zapsat jeden symbol – např. „*b*“ dvakrát, znamenalo by to, že jednak $aa = b$ a také $ab = b$, to by ovšem na základě předchozí věty znamenalo (neboť $aa = ab$), že $a = b$, což je spor, neboť prvky jsou navzájem různé. Vidíme tedy, že prvky se v řádcích (snadno nahlédneme, že též ve sloupcích) nesmí opakovat, z toho plyne, že v každém řádku i sloupci se musí vyskytovat všechny!

To nám již redukuje počet možností pouze na jednu:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tabulka 3: Cayleyho tabulka, vyplněná

Zatím jsme našli pouze strukturu „podezřelou z grupy“, ještě je nutné ukázat, že platí asociativita námi vytvořené operace. Ta skutečně platí, a můžeme tedy prohlásit, že jsme našli jedinou existující grupu stupně tři (až na izomorfizmus).

Poznámka: Čtenáře možná zarazí, že jsme neukazovali existenci inverzních prvků, ta je však vidět z tabulky. Obecně se dá ukázat, že asociativita společně s krácením (a konečností) postačuje, aby daná struktura byla grupou (viz [1], str. 3).

Na první pohled vypadá předcházející postup schůdně pro hledání grup daného řádu, nezapomeňme ovšem, že jsme hledali grupu pouze o třech prvcích. Pro vyšší počet prvků tento postup není příliš efektivní hlavně kvůli obtížnému ověřování asociativity. Samozřejmě bychom mohli pro ověření použít počítače, to bychom se však ochudili o pohled na vnitřní strukturu grup a na jejich zajímavé vlastnosti.

Podívejme se nyní na několik příkladů grup, konečných i nekonečných.

3 Příklady grup

Množina $\mathbb{Z}$ celých čísel spolu s operací sčítání tvoří grupu – sčítání celých čísel je zřejmě asociativní, sami tuto vlastnost při počítání zpaměti jistě využíváte; neutrálním prvkem je číslo 0, neboť 0 přičtená k libovolnému číslu dá opět toto číslo; k libovolnému číslu a existuje opačné číslo $-a$, neboť $a + (-a) = 0$.

Stejně tak množiny $\mathbb{Q}$, $\mathbb{R}$ spolu s operací sčítání tvoří grupu.

Množina $\mathbb{Z}$ spolu s operací násobení ovšem grupu netvoří – asociativita sice opět platí, dokonce existuje i neutrální prvek (číslo 1), ale prvky inverzní existují pouze k číslům 1 a –1.

Množiny $\mathbb{Q}, \mathbb{R}$ po vyloučení nuly spolu s násobením již grupu tvoří, neboť v těchto množinách již ke každému prvku nalezneme prvek inverzní.

Množina

$$\{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

všech celých čísel dělitelných třemi (obecně libovolným přirozeným číslem) spolu s operací sčítání tvoří grupu.

Množina všech vektorů (vektorem rozumíme množinu všech orientovaných úseček stejného směru a velikosti) v rovině spolu s operací skládání vektorů tvoří grupu – skutečně, skládání vektorů je asociativní (stačí od vektorů přejít k souřadnicím), neutrálním prvkem je nulový vektor a prvkem inverzním k danému vektoru je vektor opačný.

U následujících příkladů konečných grup můžeme využít již zmiňované Cayleyho tabulky:

Množina

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

spolu se sčítáním modulo 6 (zbytek po dělení šesti) tvoří grupu

+	0	1	2	3	4	5
0	**0**	1	2	3	4	5
1	1	2	3	4	5	**0**
2	2	3	4	5	**0**	1
3	3	4	5	**0**	1	2
4	4	5	**0**	1	2	3
5	5	**0**	1	2	3	4

Tabulka 4: Grupa zbytkových tříd modulo 6

Povšimněme si na tomto místě faktu, že kromě toho, že neutrální prvek (zde číslo 0) se musí vyskytovat v každém řádku i sloupci (plyne mj. z toho, že ke každému prvku musí existovat prvek inverzní), musí být tento navíc rozmístěn symetricky podle hlavní diagonály, neboť z rovnosti $a + b = 0$ plyne $b + a = 0$. U komutativních grup je podle hlavní diagonály symetrická celá tabulka.

Také množina komplexních čísel $\{1, -1, i, -i\}$ spolu s násobením tvoří grupu

*	1	–1	i	$-i$
1	1	–1	i	$-i$
–1	–1	1	$-i$	i
i	i	$-i$	–1	1
$-i$	$-i$	i	1	–1

Tabulka 5: Grupa $\{1, -1, i, -i\}$

Velice zajímavou grupou je rozšíření předchozí grupy, na jehož základě lze definovat rozšíření komplexních čísel, tzv. *kvaterniony*. K prvkům předchozí grupy přidáme prvky

$$j, -j, k, -k$$

a definujeme (analogicky jako u imaginární jednotky i)

$$j^2 = (-j)^2 = k^2 = (-k)^2 = -1 \ .$$

Pro vzájemné vztahy mezi prvky zavedeme násobení následovně:

$$ij = k \ , \ jk = i \ , \ ki = j \ , \ kj = -i \ , \ ji = -k \ , \ ik = -j \ .$$

Permutací na množině M nazveme libovolnou bijekci na této množině. Zapisujeme ji obvykle ve tvaru

$$P = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ P(a_1) & P(a_2) & \dots & P(a_n) \end{pmatrix}.$$

Jelikož skládání zobrazení je asociativní, složením bijekcí je opět bijekce, permutace

$$E = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

je neutrálním prvkem a permutace

$$P^{-1} = \begin{pmatrix} P(a_1) & P(a_2) & \dots & P(a_n) \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

je inverzní k permutaci P, tvoří všechny permutace n-prvkové množiny spolu s operací skládání zobrazení grupu. Tuto grupu nazýváme symetrická grupa stupně n, značíme S_n. Transpozicí rozumíme permutaci, která pouze „prohazuje“ dva prvky, tedy permutaci tvaru

$$P = \begin{pmatrix} a_1 & a_2 & \dots & a_i & \dots & a_j & \dots & a_n \\ a_1 & a_2 & \dots & a_j & \dots & a_i & \dots & a_n \end{pmatrix}.$$

Lze ukázat, že každou permutaci lze složit z transpozic. Dle toho, zde lze permutace složit z lichého, resp. sudého počtu transpozic, nazveme ji lichou, resp. sudou permutací. Zřejmě složením dvou sudých permutací je opět sudá permutace, identická permutace je sudá. Inverzní permutace k sudé permutaci je také sudá, neboť jejich složením má vzniknout sudá identická permutace. Ukázali jsme tedy, že sudé permutace tvoří podgrupu grupy S_n. Zvolíme-li pevně libovolnou lichou permutaci Q, pak zobrazení

$$f : P \to PQ; \ P \in S_n$$

je bijekcí, která zobrazuje sudé permutace na liché a naopak. Z toho vyplývá, že počty sudých a lichých permutací jsou stejné. Jelikož není permutace nic jiného než změna pořadí prvků, obsahuje grupa S_n právě $n!$ prvků. Podgrupa sudých permutací obsahuje tedy $\frac{n!}{2}$ prvků (pro $n > 1$). Této podgrupě říkáme alternující grupa stupně n, značíme ji A_n.

Permutace jsou důležité mj. i proto, že ke každé konečné grupě lze nalézt izomorfní podgrupu nějaké symetrické grupy (tvrdí to tzv. *Cayleyova věta*).

Jako poslední příklad uveďme tzv. *grupu zákrytových pohybů rovnostranného trojúhelníku*:

Existuje šest základních pohybů, kterými můžeme přemístit rovnostranný trojúhelník *ABC* na sebe:

- Identita
- Rotace podle středu o 120° po směru hodinových ručiček
- Rotace podle středu o 120° proti směru hodinových ručiček
- Osová souměrnost podle osy procházející vrcholem *C*
- Osová souměrnost podle osy procházející vrcholem *B*
- Osová souměrnost podle osy procházející vrcholem *A*

Vezmeme-li tyto pohyby za prvky množiny a jako operaci použijeme skládání těchto pohybů, získáme grupu – skládání operací je asociativní, identita je neutrálním prvkem a zároveň je sama k sobě inverzní, rotace jsou inverzní k sobě navzájem a souměrnosti jsou inverzní samy k sobě.

Pokud označíme pohyby postupně *I, R, L, C, B, A,* získáme následující Cayleyho tabulku:

	I	*L*	*R*	*A*	*B*	*C*
I	*I*	*L*	*R*	*A*	*B*	*C*
L	*L*	*R*	*I*	*B*	*C*	*A*
R	*R*	*I*	*L*	*C*	*A*	*B*
A	*A*	*C*	*B*	*I*	*R*	*L*
B	*B*	*A*	*C*	*L*	*I*	*R*
C	*C*	*B*	*A*	*R*	*L*	*I*

Tabulka 6: Grupa zákrytových pohybů trojúhelníku

4 Grupový homomorfismus

Vraťme se ještě k příkladu z předchozí části, totiž ke grupě $\{1, -1, i, -i\}$ spolu s násobením, a porovnejme ji s grupou sčítání modulo 4:

*	1	–1	*i*	–*i*
1	1	–1	*i*	–*i*
–1	–1	1	–*i*	*i*
i	*i*	–*i*	–1	1
–*i*	–*i*	*i*	1	–1

Tabulka 7: Grupa $\{1, -1, i, -i\}$

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

Tabulka 8: Grupa $\mathbb{Z}_4$

Na první pohled tabulky příliš podobně nevypadají, stačí ovšem permutovat řádky a sloupce první tabulky, abychom spatřili analogii:

*	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Tabulka 9: Grupa $\{1, -1, i, -i\}$ *po permutování řádků*

Nyní již vidíme, že řádky v obou tabulkách vypadají podobně – následující řádek vzniká z předchozího přemístěním prvního prvku na konec. Jinými slovy, můžeme ztotožnit prvky 0 a 1, 1 a i, 2 a -1, 3 a $-i$. Rozdíl mezi grupami je tedy de facto pouze v označení prvků a operací, jejich struktura je stejná. Pokusme se toto pozorování zformalizovat.

Nechť je dána grupa G s operací „$*$“ a grupa H s operací „$\circ$“. Zobrazení $f : G \to H$ nazveme homomorfismus, pokud platí

$$\forall g_1, g_2 \in G: f(g_1) \circ f(g_2) = f(g_1 * g_2).$$

Speciálně, je-li toto zobrazení prosté, resp. na, nazveme jej monomorfismus, resp. epimorfismus. Zobrazení, které je současně prosté a na nazveme izomorfismus.

Zhruba řečeno, izomorfismus znamená „přejmenování prvků a operace“. Pokud se budeme držet našeho příkladu, můžeme zavést zobrazení

$$f: \{0, 1, 2, 3\} \to \{1, -1, i, -i\}, \; f(0) = 1, f(1) = i, \; f(2) = -1, f(3) = -i.$$

Toto zobrazení je zřejmě prosté a na, z Cayleyho tabulek je vidět, že splňuje podmínku kladenou na homomorfismus, jedná se tedy o izomorfismus. Fakt, že grupa G je izomorfní s grupou H, značíme

$$G \simeq H.$$

Dalším zajímavým příkladem homomorfismu je logaritmus. Protože platí

$$\forall x, y \in (0, \infty): \log(xy) = \log(x) + \log(y),$$

je toto zobrazení homomorfismem grupy nezáporných reálných čísel spolu s operací násobení do grupy reálných čísel spolu s operací sčítání. Tento homomorfismus je navíc prostý a na (z definice logaritmu), jedná se tedy dokonce o izomorfismus (viz [4], str. 50) .

Cílem naší práce samozřejmě není najít *všechny* konečné grupy do řádu 15, neboť těch je nekonečně mnoho, bude nás zajímat pouze vnitřní struktura těchto grup, tudíž budeme hledat konečné grupy do řádu 15 „až na izomorfismus“.

5 Podgrupa

Dalším pojmem, který při zkoumání grup vyvstane, je pojem podgrupy. Stačí se podívat na levý horní roh jedné z předchozích tabulek:

	I	L	R
I	I	L	R
L	L	R	I
R	R	I	L

Tabulka 10: Podgrupa grupy zákrytových pohybů trojúhelníku

Splňuje tato část tabulky požadavky na grupu? Vidíme, že tabulka obsahuje pouze prvky *I, L, R,* operace skládání je tedy korektně definována. Asociativita platila již v původní tabulce, omezíme-li se pouze na několik prvků z ní, bude platit tím spíše. Neutrálním prvkem je opět identita, rotace jsou opět inverzní samy k sobě – tedy podmnožina $\{I, L, R\}$ původní množiny je opět grupou. A to není vše! Pokud vybereme pouze identitu spolu s libovolnou souměrností, získáme opět podgrupu, jak ukazuje následující tabulka:

	I	A
I	I	A
A	A	I

Tabulka 11: Podgrupa grupy zákrytových pohybů trojúhelníku

Takovouto „grupu uvnitř grupy“ nazveme podgrupou:

Podmnožinu H grupy G nazveme podgrupou grupy G, pokud tvoří grupu vzhledem k operaci definované v grupě G.

Jak již bylo řečeno výše, při ověřování, zda je daná podmnožina podgrupou, není nutné ověřovat první z axiomů grupy, ten je zaručen asociativitou v původní grupě.

Pokud si pozorně prohlédneme příklady grup z předešlé kapitoly, najdeme jistě další příklady podgrup – např. z grupy $\{1, -1, i, -i\}$, můžeme vytvořit podgrupu $\{1, -1\}$, vektrory v rovině lze omezit pouze na vektory stejného směru a konečně z grupy $\mathbb{Z}_6$ můžeme vybrat pouze sudá čísla:

+	0	2	4
0	**0**	2	4
2	2	4	**0**
4	4	**0**	2

Tabulka 12: Podgrupa grupy $\mathbb{Z}_6$

Poznámka: Samozřejmě můžeme za podgrupu zvolit i dva extrémní případy – grupu obsahující pouze neutrální prvek a celou původní grupu. V prvním případě hovoříme o triviální podgrupě (ostatní grupy jsou netriviální), v druhém případě hovoříme o nevlastní podgrupě (ostatní jsou vlastní).

Alternativní způsob, jak rozpoznat, zda je daná podmnožina grupy její podgrupou, přináší následující věta, nadále ji budeme označovat jako alternativní kritérium pro podgrupy:

Neprázdná podmnožina H grupy G je podgrupou právě tehdy, když s každými dvěma prvky a, b obsahuje i prvek ab^{-1}.

Implikace zleva doprava je zřejmá, neboť grupa musí obsahovat inverzní prvky i součiny prvků. Zbývá ukázat, že platí-li pravá strana tvrzení, pak množina k daným prvkům *a*, *b* obsahuje i prvky *ab* a a^{-1} a navíc obsahuje jednotku *e*. Jednotkový prvek množina obsahuje, neboť

$$e = aa^{-1}$$

(všimněte si, že zde využíváme neprázdnost podgrupy *H*), inverzní prvek a^{-1} lze vyjádřit jako $a^{-1} = ea^{-1}$. Obsahuje-li množina prvek *b*, musí tedy obsahovat i prvek b^{-1} a konečně tedy i prvek

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

což mělo být dokázáno.

Ukažme dále způsob, jak z daných podgrup grupy vytvářet podgrupy nové.

Předně platí, že průnik podgrup grupy je opět podgrupa – průnik je jistě neprázdný, neboť všechny podgrupy dané grupy musí obsahovat její neutrální prvek. Pokud průnik obsahuje prvky *a, b,* obsahují tyto prvky i všechny podgrupy, samozřejmě i spolu s prvkem ab^{-1}. Tento prvek musí být tudíž obsažen i v průniku, z čehož lze vyvodit, že průnik sám je podgrupou původní grupy. Průnik grup *A, B* budeme značit $A \cap B$.

Vraťme se ještě ke grupě $\mathbb{Z}_6$ – vybrali jsme z ní podgrupu s prvky 0, 2, a 4, označme ji *H.* Povšimněme si, že zbylé prvky můžeme získat tak, že každý prvek podgrupy zvětšíme o jedničku, tedy např. jako množinu

$$H + 1 = \{h + 1 ; h \in H\}.$$

Vytvořme nyní všechny možné takovéto množiny:

$$H + 0 = H + 2 = H + 4 = \{0, 2, 4\};\ H + 1 = H + 3 = H + 5 = \{1, 3, 5\}.$$

Důležité pro nás bude zejména následující pozorování – obě množiny mají stejný počet prvků, jsou disjunktní, jejich sjednocením je původní množina a navíc odečteme-li od sebe dva libovolné prvky z množiny $\{1, 3, 5\}$, bude rozdíl těchto prvků ležet v podgrupě *H.*

Podívejme se pro ilustraci ještě na grupu $\{1, -1, i, -i\}$, *z* níž jsme vybrali podgrupu

$$H = \{1, -1\}.$$

Zde bylo grupovou operací násobení, budeme tedy tvořit množiny $Ha = \{ha;\ h \in H\}$.

Výsledek je následující:

$$H \cdot 1 = H \cdot (-1) = \{1, -1\};\ H \cdot i = H \cdot (-i) = \{i, -i\},$$

což je, jak vidíme, analogické předchozímu příkladu.

Zkusme se zaměřit ještě na dvouprvkovou podgrupu grupy zákrytových pohybů rovnoramenného trojúhelníku, tedy na podgrupu $H = \{I, A\}$. Pro změnu budeme tentokrát násobit zleva:

$$I \cdot H = A \cdot H = \{I, A\};\ L \cdot H = B \cdot H = \{L, B\};\ R \cdot H = C \cdot H = \{R, C\}.$$

Nyní jsme získali dokonce tři množiny, platí pro ně ovšem to samé, co v předchozích příkladech.

V tomto případě platí

$$R \cdot C^{-1} = R \cdot C = B\,,$$

což ovšem není prvek podgrupy *H*. To je v pořádku, protože jsme zaměnili násobení zprava za násobení zleva, je nutné násobit v obráceném pořadí, tedy

$$R^{-1} \cdot C = L \cdot C = A\,,\ \text{případně}\ C^{-1} \cdot R = C \cdot R = A\,.$$

Předchozí úvahy nás přivádějí k dalšímu důležitému pojmu – k levé, resp. pravé třídě grupy podle podgrupy.

6 Třídy grupy podle podgrupy

Nechť je dána konečná grupa G spolu s podgrupou H. Nechť dále je a libovolný prvek grupy G. Množinu $aH = \{ah\,;\ h \in H\}$*, resp.* $Ha = \{ha\,;\ h \in H\}$ *nazveme levá, resp. pravá třída grupy G podle podgrupy H.*

Nyní dokážeme, co jsme vypozorovali v předešlých příkladech:

1. Všechny různé levé třídy jsou navzájem disjunktní a jejich sjednocení tvoří původní grupu – řekneme, že třídy tvoří rozklad grupy *G.* Totéž platí i pro pravé třídy.
2. Všechny třídy mají stejný počet prvků.
3. Prvky *a*, *b* patří do stejné levé (resp. pravé) třídy právě tehdy, pokud $a^{-1}b \in H$*,* resp. $a\,b^{-1} \in H$.

Důkaz provedeme pouze pro pravé třídy, důkaz pro levé třídy je analogický.

Ukažme nejprve, že sjednocení tříd tvoří celou původní grupu – vskutku, jelikož jednotkový prvek *e* se nutně nachází v podgrupě *H*, libovolný prvek $a \in G$ se jistě nachází ve třídě *Ha*, neboť jej lze vyjádřit jako *ea*. Jelikož se tedy tento prvek nachází v jedné z tříd, bude se nacházet i v jejich sjednocení.

Dále dokažme, že dvě různé pravé třídy jsou navzájem disjunktní, jinak řečeno – mají-li dvě třídy neprázdný průnik, jsou totožné. Nechť jsou dány dvě třídy, *Ha* a *Hb,* dále pak prvek

$$c \in (Ha \cap Hb)\,.$$

Nechť je *x* libovolný prvek z *Ha*, tedy

$$x = h_1 a\,;\ h_1 \in H\,,$$

z $c \in (Ha \cap Hb)$ ovšem plyne

$$c = h_2 a = h_3 b\,;\ h_2,\ h_3 \in H\,,$$

po vynásobení druhé rovnosti zleva prvkem h_2^{-1} získáváme $a = h_2^{-1} h_3 b$, tedy

$$x = h_1 a = h_1 h_2^{-1} h_3 b = (h_1 h_2^{-1} h_3) b = h_4 b\,;\ h_4 \in H\,.$$

Z toho je již zřejmé, že prvek *x* musí ležet i v množině *Hb,* tedy $Ha \subseteq Hb$. Analogicky lze ukázat druhou inkluzi, tedy $Ha = Hb$, což jsme chtěli ukázat.

Třídy mají stejný počet prvků – předně je jistě jedna ze tříd rovna samotné grupě *H*, neboť

$$H = He\,.$$

Ukažme, že pokud

$$h_1 \neq h_2 \ \ (h_1,\ h_2 \in H)\ ,$$

pak také $h_1 a \neq h_2 a$, neboli

$$h_1 a = h_2 a \rightarrow h_1 = h_2$$

pro libovolný prvek a z grupy *G*. Stačí ovšem první nerovnost zprava vynásobit a^{-1} a okamžitě vidíme, že tvrzení platí. Tedy různé prvky grupy *H* jsou zobrazovány na různé prvky třídy *Ha*, což (v případě konečnosti grupy *G*) zaručuje, že $|H| = |Ha|$.

Třetí tvrzení je ekvivalence, nejprve ukažme implikaci zleva doprava:

Nechť prvky *a*, *b* patří oba do stejné třídy ekvivalence *xH*, jdou tedy vyjádřit ve tvaru

$$a = x\,h_1,\ b = x\,h_2\ ,\ \text{potom však}$$

$$a^{-1}b = (x\,h_1)^{-1}\,x\,h_2 = h_1^{-1}\,x^{-1}\,x\,h_2 = h_1^{-1}h_2 \in H\ .$$

Obráceně, nechť $a^{-1}b \in H$, tedy $a^{-1}b = h_1$. Pokud např. prvek a leží ve třídě *xH*, pak zřejmě

$$a = x\,h_2\ .$$

Následkem toho ovšem i

$$b = a h_1 = (x\,h_2)\,h_1 = x\,(h_2 h_1) = x\,h_3 \in xH\ .$$

Dokázali jsme, že prvky *a*, *b* patří do stejné třídy ekvivalence *xH* právě tehdy, když platí

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

Počtu levých (a jak je zřejmé z toho, že $|aH| = |H| = |Ha|$, i pravých) tříd konečné grupy *G* podle podgrupy *H* budeme říkat index podgrupy *H v* grupě *G*, značíme $[G:H]$.

Předcházejí úvahy nás přivádějí k velice užitečné větě (*Lagrange*):

Nechť je dána konečná grupa G a její podgrupa H. Potom řád (počet prvků) podgrupy H dělí řád grupy G, přesněji $|G| = [G:H] \cdot |H|$.

Důkaz vyplývá z toho, že grupa je disjunktním sjednocením množin, které mají stejný počet prvků jako podgrupa *H*.

Poznamenejme, že požadavek na řád, plynoucí z Lagrangeovy věty, je obecně pouze nutnou podmínkou pro existenci podgrupy, tj. ne pro každé číslo dělící řád grupy existuje podgrupa daného řádu. Postačující podmínku nám poskytnou Sylowovy věty, ke kterým se dále dostaneme.

7 Normální podgrupa

Při vyšetřování levých tříd grupy zákrytových pohybů rovnostranného trojúhelníku dle podgrupy

$$H = \{I,\ A\}$$

jsme získali rozklad

$$I \cdot H = A \cdot H = \{I,\ A\};\ L \cdot H = B \cdot H = \{L,\ B\};\ R \cdot H = C \cdot H = \{R,\ C\}\ .$$

Pokud bychom zkusili udělat rozklad na pravé třídy, získáme následující:

$$H \cdot I = H \cdot A = \{I,\ A\};\ H \cdot L = H \cdot C = \{L,\ C\};\ H \cdot R = H \cdot B = \{R,\ B\}\ .$$

Jak vidíme, rozklady na levé a pravé třídy dle stejné podgrupy se obecně nemusí shodovat. Pro nás by samozřejmě bylo výhodnější, kdyby nám podgrupa jednoznačně určila rozklad bez ohledu na to, zda násobíme zleva či zprava. Jaké požadavky musí tedy podgrupa splňovat, aby $aH = Ha$ pro každý prvek $a \in G$? Pokud má prvek x ležet zároveň v obou třídách, musí platit, že

$$x = a\,h_1 = h_2\,a \text{ , tedy}$$

$$h_1 = a^{-1} h_2\,a\,;\; a \in G\,;\; h_1,\; h_2 \in H\,.$$

Obráceně, pokud platí $a^{-1} h_2\,a \in H$, tak $ah_1 = h_2\,a$ a tedy $aH = Ha$. Nyní již můžeme definovat normální (dle [2], str. 80 též invariantní) podgrupu:

Podgrupu H grupy G nazveme normální podgrupou grupy G, pokud platí:

$$\forall\, a \in G\,,\; \forall\, h \in H\,;\; a^{-1} h\,a \in H\,.$$

Je-li H normální podgrupou grupy G, píšeme $H \lhd G$.

Snadno se ukáže, že lze použít i definici

$$\forall\, a \in G\,,\; \forall\, h \in H\,;\; a\,h\,a^{-1} \in H$$

(stačí $a^{-1} ha$ přepsat ve tvaru $(a^{-1})\,h\,(a^{-1})^{-1}$).

Zřejmě triviální i nevlastní podgrupa jsou normální, navíc každá podgrupa komutativní grupy je normální, neboť

$$aha^{-1} = a\,a^{-1} h = h \in H\,.$$

Dospěli jsme tedy k závěru, že rozklad podle speciální, tzv. *normální podgrupy* je stejný, ať zvolíme levé či pravé třídy. Pro ilustraci si vezměme množinu celých čísel spolu se sčítáním a její podgrupu

$$3\mathbb{Z} = \{3z\,;\; z \in \mathbb{Z}\}\,.$$

(Grupa i podgrupa jsou samozřejmě nekonečné, ale dle autora tento příklad dobře vystihuje důvod rozkladu množiny na třídy, proto byl zařazen.) Protože grupa $\mathbb{Z}$ je komutativní, její podgrupa $3\mathbb{Z}$ je normální. Tato podgrupa nám množinu celých čísel rozloží na tři disjunktní podmnožiny

$$3\mathbb{Z} = \{\ldots,\, -9, -6, -3,\, 0,\, 3,\, 6,\, 9,\, \ldots\};\; 3\mathbb{Z} + 1 = \{\ldots,\, -8, -5, -2,\, 1,\, 4,\, 7,\, 10,\, \ldots\}$$

$$3\mathbb{Z} + 2 = \{\ldots,\, -7, -4, -1,\, 2,\, 5,\, 8,\, 11,\, \ldots\}\,.$$

Povšimněme si následujícího – pokud budeme sčítat dva prvky z různých podmnožin, nezáleží, jak konkrétně tyto prvky zvolíme, výsledek se vždy bude nacházet ve stejné množině, např.

$$-5 + 8 = 3 \in 3\mathbb{Z}\,,\; 10 - 1 = 9 \in 3\mathbb{Z}\,,\; \ldots$$

Nabízí se tedy myšlenka zavést přímo „sčítání podmnožin“, tedy de facto od množiny celých čísel přejít k tříprvkové množině

$$\{3\mathbb{Z},\; 3\mathbb{Z} + 1,\; 3\mathbb{Z} + 2\}\,.$$

Ukáže se, že takovéto „sčítání podmnožin“ má vlastnosti grupové operace.

8 Faktorizace podle normální podgrupy

Nechť je tedy dána grupa *G a* její normální podgrupa *H*. Při rozkladu získáme třídy tvaru *aH*, které bychom rádi považovali za prvky nové grupy. K tomu ovšem musíme nejprve definovat operaci násobení tříd. Podíváme-li se na předchozí příklad, zjistíme, že účelné bude vzít za součin tříd *aH* a *bH* třídu, ve které leží součin prvků *ab*, tedy třídu *abH*.

Aby toto nové násobení bylo korektně definováno, musí být zaručeno, že zvolíme-li jiné reprezentanty tříd, dostaneme stejný výsledek, jinak řečeno, pokud

$$a_1 H = a_2 H\,,\; b_1 H = b_2 H\,,$$

pak musí platit $(a_1 b_1) H = (a_2 b_2) H$. To však vskutku platí: jestliže

$$a_1 H = a_2 H\,,\; b_1 H = b_2 H\,,$$

pak $a_1^{-1} a_2,\; b_1^{-1} b_2 \in H$; chceme ukázat, že $(a_1 b_1)^{-1} a_2 b_2 \in H$, po úpravě dostaneme

$$(a_1 b_1)^{-1} a_2 b_2 = b_1^{-1}(a_1^{-1} a_2) b_2 = b_1^{-1} h_1 b_2 = b_1^{-1} h_1 (b_1 b_1^{-1}) b_2 = (b_1^{-1} h_1 b_1)(b_1^{-1} b_2) = h_2 h_3 \in H$$

– všimněme si, že v posledním kroku potřebujeme, aby daná podgrupa byla normální, pak totiž prvek $b_1^{-1} h_1 b_1$ leží v grupě *H*.

Nyní již víme, že operace násobení tříd je korektně definována, dále je třeba ověřit axiomy grupy. Uzavřenost je zřejmá, jelikož násobení tříd není ničím jiným než násobením reprezentantů, platí asociativita, neutrálním prvkem je třída *eH = H*, tedy původní podgrupa, inverzním prvkem ke třídě *aH* je třída $a^{-1}H$.

Takto definovanou grupu budeme nazývat faktorová grupa grupy *G* podle normální podgrupy *H*, značíme *G/H*.

Naznačené dělení v označení evokuje jednak fakt, že grupa *G* je podgrupou opravdu „rozdělena“ na jednotlivé třídy, jednak u konečných grup vypovídá i o počtu prvků nové grupy, který je roven číslu

$$|G|/|H|\,.$$

9 Transformace, konjugované podgrupy

V definici normální podgrupy jsme hovořili o podmínce

$$\forall\, a \in G\;\; \forall\, h \in H\colon a^{-1} h a \in H\,.$$

Jinak řečeno, požadovali jsme, aby poté, co na prvek podgrupy zprava, resp. zleva „aplikujeme“ libovolný prvek grupy, resp. jeho inverzi, výsledek stále náležel do původní grupy. Tento koncept nyní zobecněme:

Transformací prvku b prvkem a rozumíme prvek $b^a = a^{-1} b a$. *Dva prvky grupy nazveme konjugovanými, je-li jeden z nich transformací druhého (libovolným prvkem grupy). Transformací podgrupy H grupy G prvkem rozumíme množinu* $H^g = \{g^{-1} h g\,;\, h \in H\}$.

Je patrné, že každý prvek je konjugován sám se sebou ($a^e = a$). Dále je relace konjugovanosti symetrická, neboť z $a = b^x$, tj. plyne

$$b = x a x^{-1}\,,\text{ tj. }\; b = a^{x^{-1}}\,.$$

Konečně ukažme tranzitivitu – z rovností

$$a = x_1^{-1} b\, x_1\,,\; b = x_2^{-1} c\, x_2$$

odvodíme

$$a = x_1^{-1} x_2^{-1} c\, x_2 x_1 = (x_2 x_1)^{-1} c\, x_2 x_1 = c^{x_2 x_1}\,.$$

Relace konjugovanosti je tedy ekvivalence, která nám danou grupu rozdělí na množiny vzájemně konjugovaných prvků.

Vraťme se k příkladu se zákrytovými pohyby rovnostranného trojúhelníku. Zjistili jsme, že podmnožina $H = \{I\,,\; A\}$ je podgrupou naší grupy. Zkusme vytvořit konjugované množiny:

$$H^I = H^A = H\,,\; H^B = H^R = \{I\,,\; C\},\; H^C = H^L = \{I\,,\; B\}\,.$$

Povšimněme si následujícího – nejen že nám po transformaci vyšla množina se shodným počtem prvků, tato množina je (spolu s původní operací) podgrupou původní grupy! Ukažme, že jev pozorovaný na tomto příkladu platí obecně a nadto jsou všechny získané podgrupy izomorfní:

Nechť je dána grupa G *a* její podgrupa H. Předně je množina $H^a;\, a \in G$ jistě podgrupou, neboť s každými dvěma prvky $b_1 = a^{-1} h_1 a\,,\; b_2 = a^{-1} h_2 a$ obsahuje H^a také prvek $b_1 b_2^{-1}$, neboť

$$b_1 b_2^{-1} = a^{-1} h_1 (a\, a^{-1}) h_2 a = a^{-1} (h_1 h_2) a = a^{-1} h_3 a;\; h_3 \in H\,.$$

Jsou-li prvky $a^{-1} h_1 a$ a $a^{-1} h_2 a$ totožné, pak jsou nutně totožné i prvky h_1 a h_2 (plyne z možnosti krácení). Různým prvkům jsou tedy při transformaci grupy přiřazeny různé prvky, tudíž jejich počet musí být stejný. Zbývá ukázat, že definované zobrazení je izomorfizmus. To, že dané zobrazení je prosté, jsme právě ukázali, že je to zobrazení na je zřejmé.

Protože navíc platí

$$a^{-1} h_1 h_2 a = a^{-1} h_1 a\, a^{-1} h_2 a\,,$$

jedná se skutečně o izomorfizmus.

Transformací podgrupy vznikne opět podgrupa, a to podgrupa izomorfní s původní podgrupou.

Nyní, když víme, že z podgrupy získáme transformací opět podgrupu, můžeme zavést následující definici:

Řekneme, že podgrupy H_1, H_2 jsou (vzájemně) konjugované, vznikne-li jedna z nich transformací druhé.

Můžeme si dovolit napsat „vzájemně“, neboť se snadno ověří, že pokud je H_2 transformací H_1 prvkem a, tak je H_1 transformací H_2 prvkem a^{-1}, protože

$$(a^{-1})^{-1} (a^{-1} h\, a)(a^{-1}) = h\,.$$

Vrátíme-li se k definici normální podgrupy, zjistíme, že při její transformaci libovolným prvkem získáme opět tu samou podgrupu. U obecné podgrupy to samozřejmě pro libovolný prvek nenastane, ukážeme ovšem, že prvky, které podgrupu transformují na sebe samu, tvoří podgrupu:

Nechť je dána podgrupa H grupy G. Pokud $H^a = H$, pak ke každému prvku $h \in H$ nutně existuje $h_1 \in H$, že $a^{-1} h_1 a = h$, tedy

$$h_1 = a\,h\,a^{-1} = (a^{-1})^{-1} h\,a^{-1},$$

z čehož vyplývá, že

$$H^{(a^{-1})} \subseteq H.$$

Naopak, je-li $h \in H$, lze jej vyjádřit jako

$$h = a(a^{-1} h\,a)a^{-1} = (a^{-1})^{-1} h_1 a^{-1},$$

z čehož vyplývá obrácená inkluze. Spojením obou inkluzí získáváme tvrzení, že z $H^a = H$ plyne $H^{(a^{-1})} = H$ (viz [5], str. 97).

Tohoto pomocného tvrzení nyní využijeme k dokončení důkazu – platí-li

$$H^a = H,\ H^b = H, \text{ pak i}$$

$$H^{(ab^{-1})} = \{(ab^{-1})^{-1} h(ab^{-1});\ h \in H\} = \{b(a^{-1} h\,a)b^{-1};\ h \in H\} = (H^a)^{(b^{-1})} = H,$$

tedy dle alternativního kritéria pro podgrupy tvoří množina $N(H) = \{a \in G;\ H^a = H\}$ podgrupu grupy G. Tuto grupu nazveme *normalizátorem podgrupy H*.

Normalizátorem normální podgrupy je tedy zřejmě celá původní grupa. Obecně platí inkluze

$$H \subseteq N(H),$$

vyplývá to z uzavřenosti grupové operace. Nadto platí i $H \lhd N(H)$. Lze říci, že normalizátor grupy H *v* grupě G je největší podgrupa K grupy G taková, že $H \lhd K$.

Pokud si pozorně prohlédneme naznačený důkaz, zjistíme, že jsme vlastně nikde nevyužívali předpokladu, že množina H je podgrupou grupy G. Lze tedy stejně tak hovořit o *normalizátoru podmnožiny H,* resp. o *normalizátoru prvku x,* píšeme

$$N(x) = \{a \in G;\ x^a = x\}.$$

To, že $H^a = H$ samozřejmě ještě neznamená, že by se každý prvek zobrazil sám na sebe. Pokud toto budeme požadovat, obdržíme množinu

$$C(H) = \{a \in G;\ \forall\, h \in H : h^a = h\},$$

kterou nazveme *centralizátorem podgrupy H*, speciálně, pokud $G = H$, hovoříme o *centru grupy G*. Zřejmě je centralizátor podmnožinou odpovídajícího normalizátoru, analogicky jako v případě normalizátoru se ukáže, že je dokonce podgrupou.

Již jsme zmínili, že relace konjugovanosti prvků grupy je ekvivalencí, která grupu rozdělí na třídy vzájemně konjugovaných prvků. Ukažme nyní na dvou příkladech, jak budou tyto třídy vypadat:

Jako první příklad použijeme grupu sčítání modulo 6, tedy grupu $\mathbb{Z}_6$. Snadno nahlédneme, že tato grupa se nám rozpadne na šest jednoprvkových tříd, neboť

$$\forall\, a,\ b \in G;\ -b + a + b = a + (-b) + b = a + 0 = a.$$

Je též patrné, že tento triviální případ nastal proto, že grupa $\mathbb{Z}_6$ je Abelovská. Zkusme nyní vyšetřovat grupu zákrytových pohybů rovnostranného trojúhelníku, o níž víme, že není komutativní. Získáme následující rozklad:

$$G_I = \{I\},\ \{A,\ B,\ C\},\ \{L,\ R\}.$$

Vidíme, že neutrální prvek je konjugován pouze sám se sebou – to ovšem není překvapivé, neboť zřejmě platí

$$\forall\, a \in G;\ e^a = a^{-1} e a = a^{-1} a = e\ .$$

Obecněji, pokud je nějaký prvek grupy konjugován pouze sám se sebou, musí platit

$$\forall\, x \in G;\ a^x = a\ \text{, tedy}\ \ \forall\, x \in G;\ x^{-1} a x = a\ \text{, resp.}\ \ \forall\, x \in G;\ ax = xa\ .$$

Snadno nahlédneme, že poslední rovnost není nic jiného, než podmínka, aby prvek a patřil do centra grupy *G*. Lze tedy říci, že do centra grupy patří právě prvky, které jsou konjugovány pouze samy se sebou.

Ukažme nyní další zajímavou vlastnost, které jsme si mohli povšimnout u příkladu – počty prvků tříd konjugovaných prvků dělí řád grupy. Při důkazu využijeme pojmu normalizátor prvku:

Nechť je dán libovolný prvek *a* grupy *G*, jeho normalizátorem je podgrupa $N(a)$ původní grupy. Podívejme se, kdy budou dva prvky vzniklé transformací prvku *a* shodné (viz [6], str. 14):

$$a^x = a^y \Leftrightarrow x^{-1} a\, x = y^{-1} a\, y \Leftrightarrow a = (yx^{-1})\, a\, xy^{-1} \Leftrightarrow a = (xy^{-1})^{-1} a\, (xy^{-1}) \Leftrightarrow a = a^{x y^{-1}} \Leftrightarrow$$

$$\Leftrightarrow xy^{-1} \in N(a) \Leftrightarrow x = N(a)\, y\ .$$

Vidíme tedy, že transformované prvky jsou shodné právě tehdy, když transformující prvky leží ve stejné pravé třídě rozkladu dle příslušného normalizátoru. Jinými slovy – počet navzájem různých konjugovaných prvků s prvkem *a* je roven indexu normalizátoru $N(a)$ v grupě *G*, což je číslo, které (dle Lagrangeovy věty) dělí řád grupy *G*.

Na základě zjištěných poznatků lze vyvodit následující (tzv. *třídová rovnice*):

Řád konečné grupy *G* lze psát ve tvaru součtu

$$|G| = 1 + x_1 + x_2 + \ldots + x_r;\ r \in \mathbb{N}\ ,$$

kde všechny sčítance odpovídají počtu prvků ve třídách vzájemně konjugovaných prvků (číslo 1 reprezentuje třídu obsahující pouze neutrální prvek). Tyto sčítance dělí řád grupy, neboť odpovídají též indexům jistých podgrup (normalizátorů) (viz [7], str. 80).

Alternativně lze řád vyjádřit též ve tvaru

$$|G| = c + x_1 + x_2 + \ldots + x_q;\ q \in \mathbb{N}\ ,$$

kde číslo *c* odpovídá řádu centra, tedy počtu jednoprvkových tříd rozkladu na vzájemně konjugované prvky.

U předchozího příkladu se obě tyto rovnice konkretizují na $6 = 1 + 2 + 3$.

Ukázali jsme, že počet prvků konjugovaných s daným prvkem je roven indexu normalizátoru daného prvku, toto tvrzení však platí i v obecnější podobě – je-li dána podgrupa *H* grupy *G*, pak počet podgrup konjugovaných s podgrupou *H* je roven indexu normalizátoru podgrupy *H* v grupě *G*.

10 Cyklická grupa

Vraťme se ještě k příkladu se zákrytovými zobrazeními rovnostranného trojúhelníku. Podívejme se, co se stane, vybereme-li nějaký prvek spolu s jeho mocninami. Zvolme například rotaci proti směru hodinových ručiček, v příkladu označenou *R*, a tvořme její mocniny:

$$R^1 = R\,,\ R^2 = R \cdot R = L\,,\ R^3 = I\,,\ (R^4 = R^1 = R\,).$$

Získali jsme množinu $\{R, L, I\}$, což, jak jsme ukázali dříve, je podgrupa původní grupy! Pokud bychom zvolili např. prvek A, dostali bychom množinu $\{A, A^2 = I\}$, což je také podgrupa původní grupy.

Do třetice, zvolme číslo 5 grupy $\mathbb{Z}_6$ s operací sčítání modulo 6, získáváme:

$$5,\ 5 + 5 = 4,\ 5 + 5 + 5 = 3,\ 5 + 5 + 5 + 5 = 2,\ 5 + 5 + 5 + 5 + 5 = 1\,,$$

tedy opět podgrupu (byť nevlastní) původní grupy.

To nás vede k následující domněnce, kterou zformulujeme jako větu a posléze dokážeme:

Nechť G je konečná grupa, a její libovolný prvek. Potom množina $H = \{a^i;\ i \in \mathbb{N}\}$ *mocnin prvku a tvoří podgrupu grupy G.*

K důkazu použijeme větu o alternativním kritériu pro podgrupy, tedy ukážeme, že množina H s prvky a, b obsahuje i prvek ab^{-1}. Skládáním mocnin prvku a nám samozřejmě opět vyjdou mocniny prvku a, jediným problémem je ukázat, zda se v množině budou vyskytovat také inverzní prvky. Ukažme existenci prvku a^{-1} – je-li $a = e$ je tvrzení zřejmé, v opačném případě (vzhledem ke konečnosti grupy G) existují dvě různá kladná čísla r, s taková, že $a^r = a^s$. Nechť $r > s$. Pak

$$a^{r-s} = e,\ a^{r-s-1} = a^{-1}\,,$$

tedy jednotkový prvek, resp. prvek a^{-1} se dají vyjádřit jako kladná, resp. nezáporná mocnina prvku a.

Takovouto podgrupu (obecně i grupu), utvořenou pouze z mocnin jednoho jejího prvku, nazveme *cyklickou podgrupou* grupy, onen prvek nazveme *generátorem* cyklické podgrupy.

Z dosavadních poznatků můžeme vyvodit závěr, který bude prvním významným krokem při naší klasifikaci grup malých řádů:

Každá grupa prvočíselného řádu je cyklická.

K důkazu použijeme hlavně Lagrangeovu větu. Nechť je dána konečná grupa G, $|G| > 1$. Vezměme libovolný prvek $a \neq e$, a zkoumejme řád podgrupy tímto prvkem generované (označme ji H). Jelikož dle Lagrangeovy věty musí $|H|$ dělit $|G|$, pak (s přihlédnutím k tomu že $|G|$ je prvočíslo) nutně buď $|H| = 1$, nebo $|H| = |G|$. První možnost ovšem můžeme vyloučit, neboť podgrupa H jistě obsahuje alespoň dva prvky (a, e), tedy libovolný prvek (různý od jednotkového) generuje celou grupu G.

Jak tedy konkrétně vypadá konečná grupa prvočíselného řádu p? Vezměme nějaký nejednotkový prvek a tvořme jeho mocniny. Prvky

$$a\,,\ a^2,\ \ldots\,,\ a^{p-2},\ a^{p-1}$$

musí být navzájem různé a také různé od e (jinak bychom se při generování prvků „zacyklili“ a prvek a by nemohl generovat celou grupu). Chybí nám ještě jednotkový prvek, musí tedy platit $e = a^p$. Poznamenejme ještě, že tyto grupy nemají žádné podgrupy kromě podgrupy triviální a nevlastní.

Zobecněme nyní naše pozorování na cyklické grupy libovolného konečného řádu, tedy na grupy s prvky

$$a\,,\ a^2,\ \ldots\,,\ a^{n-2},\ a^{n-1};\ n \in \mathbb{N}\,.$$

Takovéto grupy samozřejmě mohou mít netriviální podgrupu, ta ovšem musí být opět cyklická – podgrupa H cyklické grupy zřejmě musí obsahovat pouze mocniny prvku a. Označme nejmenší z těchto mocnin k. Každý prvek podgrupy H lze vyjádřit ve tvaru a^m. Toto mocninu můžeme přepsat jako

$$a^m = a^{kp} a^q;\ 0 \le q < k,\ p \in \mathbb{N},\ q \in \mathbb{N}_0 .$$

Jelikož a^m, a^{kp} jsou prvky podgrupy, musí platit i vztah $a^q \in H$. Z nerovnosti $0 \le q < k$ vyplývá $q = 0$, a tedy každý prvek podgrupy H lze vyjádřit ve tvaru a^{kp}.

I pro cyklické grupy samozřejmě platí Lagrangeova věta, tedy řády případných (teď už víme, že cyklických) podgrup musí dělit řád grupy původní. Tedy Lagrangeova věta nám dává jakousi nutnou podmínku pro podgrupy. Ukažme, že v případě cyklických grup je tato podmínka i postačující, tj. že pokud m dělí řád grupy n, pak grupa nutně obsahuje (cyklickou) podgrupu řádu m. Nadto ukažme, že tato podgrupa je právě jedna.

Opravdu – pokud $m|n$, tak $n = mk$, a prvky e, a^k, … , $a^{(m-1)k}$ tvoří grupu o m prvcích (plyne z toho, že

$$a^{mk} = a^n = e,\ a^{kr} \cdot a^{ks} = a^{k(r+s)},\ (a^{kr})^{-1} = a^{k(m-r)}).$$

Nechť a^t, $t > k$, tvoří také grupu o m prvcích, pak zřejmě $a^{tm} = 1$, tedy $tm = xn$. Vezmeme-li v úvahu též rovnost $km = n$, pak po vydělení posledních dvou rovnic vychází, že t je násobkem k. To ale znamená, že podgrupa generovaná a^t je podgrupou podgrupy generované a^k. z rovnosti počtu prvků plyne, že grupy musí být totožné.

Při počítání s prvky cyklické grupy neděláme v podstatě nic jiného, než sčítání a odčítání exponentů, přičemž n prohlašujeme rovné 0. Proto můžeme od grupy s prvky

$$a^i;\ i = 1, \dots , n ,$$

snadno přejít k již zmiňované grupě $\mathbb{Z}_n$ spolu s operací sčítání modulo n. Přesně řečeno, zavádíme izomorfizmus

$$f : a^i \to i .$$

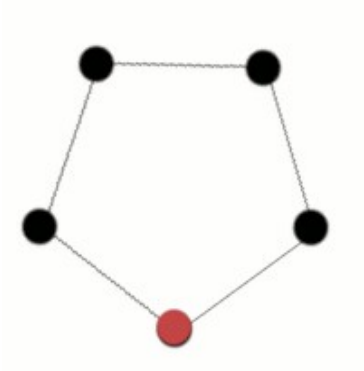
Konečně dodejme, že cyklické grupy jsou komutativní, neboť

$$a^m \cdot a^n = a^{(m+n)} = a^{(n+m)} = a^n \cdot a^m .$$

Co se týče našeho úkolu (klasifikace grup do řádu 15), podařilo se nám odhalit strukturu grup řádů 2, 3, 5, 7, 11 a 13. Tu samozřejmě můžeme vyjádřit pomocí Cayleyho tabulek, případně lze využít tzv. *grafy cyklů*.

+	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: Cyklická grupa $\mathbb{Z}_5$, Cayleyho tabulka



Obrázek 1: Cyklická grupa $\mathbb{Z}_5$, graf cyklů

Graf cyklů grupy, jak už název napovídá, zachycuje primárně cyklické podgrupy v dané grupě obsažené. Vrcholy grafu odpovídají prvkům grupy, cykly sestávají z po sobě následujících mocnin jednoho prvku, zde tedy z prvků

$$a,\ a^2,\ a^3,\ a^4,\ a^5 = e\,.$$

Násobná hrana u dvouprvkového cyklu se neznačí, neutrální prvek je zvýrazněn. Poznamenejme, že v tomto případě graf samozřejmě obsahuje pouze jeden cyklus.

11 Vlastnosti homomorfismu

Řekli jsme již, že homomorfismus je takové zobrazení jedné grupy do druhé, které zachovává definované operace. Též můžeme říct, že zachovává grupovou strukturu (ostatně slovo homomorfismus pochází ze slov „stejná struktura“ [W2]). Ukázali jsme příklad homomorfismu (dokonce izomorfismu) grupy $\mathbb{Z}_4$ spolu se sčítáním na grupu $\{1, -1, i, -i\}$ spolu s násobením:

$$f: \{0, 1, 2, 3\} \to \{1, -1, i, -i\}\ ,\ f(0) = 1,\ f(1) = i\,,\ f(2) = -1,\ f(3) = -i\,.$$

Jak vidíme, neutrální prvek první grupy se zobrazil na neutrální prvek grupy druhé. Platí to obecně, neboť zřejmě

$$f(e) = f(ee) = f(e)f(e)\,,$$

a dále můžeme psát

$$e' = f(e)(f(e))^{-1} = f(e)f(e)(f(e))^{-1} = f(e)e' = f(e)\,,$$

kde e' je neutrální prvek druhé grupy (viz [3], str. 29). Kromě toho se prvky vzájemně inverzní zobrazily na prvky vzájemně inverzní

$$(\,2 + 2 = 0 \wedge (-1)\cdot(-1) = 1\,;\ 1 + 3 = 0 \wedge i\cdot(-i) = 1\,).$$

I tento jev nastává obecně, neboť

$$f(a)f(a^{-1}) = f(aa^{-1}) = f(e) = e'\text{, a tedy } f(a^{-1}) = (f(a))^{-1}\,.$$

Ukázali jsme, že neutrální prvek se zobrazí opět na neutrální prvek, to ovšem neznamená, že na neutrální prvek se nemohou zobrazit i jiné prvky. Dokonce můžeme definovat homomorfismus, který všechny prvky jedné grupy zobrazí na neutrální prvek grupy druhé. Množině prvků, které se zobrazí na neutrální prvek, říkáme jádro homomorfismu, množině obrazů všech prvků říkáme obraz homomorfismu.

Nechť jsou dány grupy G, H a homomorfismus $f : G \to H$. *Množinu*

$$Ker\, f = \{a \in G;\ f(a) = e'\}$$

nazveme jádrem homomorfismu, množinu

$$Im\, f = \{f(a);\ a \in G\}$$

obrazem homomorfismu.

Jak nyní ukážeme, jádro homomorfismu, resp. obraz homomorfismu, je normální podgrupou, resp. podgrupou, odpovídající grupy.

Dle alternativního kritéria pro podgrupy je jádro homomorfismu podgrupou – jistě

$$e \in Ker\, f,$$

tedy jádro je neprázdné, navíc je-li $f(a) = f(b) = e'$, pak

$$f(ab^{-1}) = f(a)(f(b))^{-1} = e'(e')^{-1} = e' \in Ker\, f.$$

k tomu pro libovolný prvek *g* původní grupy a prvek a jádra homomorfismu platí

$$f(g^{-1}ag) = f(g^{-1})f(a)f(g) = f(g^{-1})e'f(g) = (f(g))^{-1}f(g) = e' \in Ker\, f,$$

tudíž jádro homomorfismu je normální podgrupou.

Co se týče obrazu homomorfismu, je také neprázdný, neboť původní grupa je neprázdná. Pokud platí $a',\ b' \in Im\, f$ existují v původní grupě prvky *a, b* takové, že

$$f(a) = a',\ f(b) = b'.$$

Pak musí být v této grupě i prvek ab^{-1}, jehož obrazem je

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = a'(b')^{-1} \in Im\, f.$$

To dokazuje, že obraz homomorfismu je podgrupou.

12 Direktní součin

Zatím umíme v dané grupě nalézt podgrupy a v případě, že se jedná o podgrupy normální, dokážeme vytvořit faktorovou grupu grupy. Přirozeným požadavkem je opačný postup, tj. tvorba „větší“ grupy z „menších“ grup. K tomu zavedeme operaci direktního součinu grup (viz [6], str. 32–34). Jsou-li dány dvě grupy, *A* a *B, a* chceme-li pomocí nich vytvořit grupu vyššího řádu, přímo se nabízí vzít za novou množinu prvků kartézský součin množiny prvků grupy *A s* množinou prvků grupy *B*. Označíme-li řády uvažovaných grup postupně *p, q*, získáme množinu

$$G = A \times B = \{(a,\ b);\ a \in A,\ b \in B\},$$

mající *pq* prvků.

Zkusme dále definovat na množině těchto uspořádaných dvojic následující násobení (poznamenejme, že a_1a_2, resp. b_1b_2 jsou součiny definované v grupě *A,* resp. *B*):

$$\forall\, a_1,\ a_2 \in A\ b_1,\ b_2 \in B: (a_1,\ b_1)(a_2,\ b_2) = (a_1a_2,\ b_1b_2).$$

Právě definovaná množina spolu s daným násobením tvoří grupu – množina je zřejmě neprázdná, asociativita plyne z asociativity v dílčích grupách, neutrálním prvkem je prvek (1, 1), prvkem inverzním k prvku (*a*, *b*) prvek (a^{-1}, b^{-1}). Pokud ztotožníme prvky grupy *A* s prvky tvaru (*a*, 1), můžeme říci, že grupa *G* obsahuje původní podgrupu *A,* analogickou úvahu lze samozřejmě provést pro prvky grupy *B a* uspořádané dvojice (1, *b*). Obě podgrupy

jsou navíc ve vytvořené grupě G normální – máme ukázat, že

$$\forall c \in A \times B,\ \forall a \in A;\ a^c \in A \text{, tedy}$$
$$\forall (a_1,\ b_1) \in A \times B,\ \forall a \in A;\ (a_1,\ b_1)^{-1}(a,\ 1)(a_1,\ b_1) \in A .$$

Poslední výraz je po úpravě roven

$$(a_1^{-1},\ b_1^{-1})(a,\ 1)(a_1,\ b_1) = (a_1^{-1} a a_1,\ 1) ,$$

což je zjevně prvek grupy A. Ukázali jsme, že grupa A je normální podgrupou grupy G, tutéž vlastnost lze ukázat i pro grupu B. Dodejme ještě, že průnikem grup $A,\ B$ je právě neutrální prvek (1, 1).

Umíme tedy vytvořit direktní součin grup, lze však postupovat obráceně, tj. danou grupu rozložit v direktní součin dvou jejích podgrup? Obecně samozřejmě ne, ukazuje se však, že právě popsané vlastnosti podgrup jsou nutné a postačující pro vytvoření direktního rozkladu, jak udává následující věta:

Grupa G je izomorfní direktnímu součinu dvou svých podgrup A, B právě tehdy, když

1. *A, B jsou normální v G*
2. $A \cap B = 1$
3. $A \cdot B = \{ab : a \in A,\ b \in B\} = G$

Implikace zleva doprava je zřejmá z definice direktního součinu, ukažme implikaci opačnou. Již na počátku řekněme, že bychom chtěli definovat izomorfismus $f : G \to A \cdot B$. K tomu uvažme prvek $a^{-1}b^{-1}ab$. Ten lze vyjádřit ve tvaru $(a^{-1}b^{-1}a)b$, resp. $a^{-1}(b^{-1}ab)$, z čehož lze vzhledem k normalitě podgrup A, resp. B vyvodit, že leží v průniku. Protože však je průnik triviální, platí $a^{-1}b^{-1}ab = 1$, neboli $ab = ba$. Zatím víme, že libovolný prvek grupy G lze vyjádřit ve tvaru

$$g = x_1 x_2 \ldots x_n;\ x_i \in A \cup B .$$

Dle právě dokázaného lze ovšem koeficienty přeskládat do tvaru, kde nejdříve bude součin prvků podgrupy A následován součinem prvků podgrupy B, formálně

$$g = a_1 \ldots a_p b_1 \ldots b_q;\ a_i \in A,\ b_i \in B .$$

Jelikož součin prvků grupy leží v grupě, lze poslední rovnost přepsat jako

$$g = ab;\ a \in A,\ b \in B .$$

Každý prvek grupy lze tedy vyjádřit ve tvaru součinu prvků podgrup, abychom mohli definovat zobrazení, potřebujeme též jednoznačnost vyjádření. Nechť $a_1 b_1 = a_2 b_2$, čili $a_2^{-1} a_1 = b_2 b_1^{-1}$. Tato rovnost neříká nic jiného, než že určitý prvek lze vyjádřit jak pomocí prvků podgrupy A, tak pomocí prvků druhé podgrupy, leží tedy v průniku. Z triviálnosti průniku vyplývá $a_2^{-1} a_1 = b_2 b_1^{-1} = 1$, z čehož plyne $a_1 = a_2,\ b_1 = b_2$. Každý prvek grupy G lze tedy jediným způsobem vyjádřit jako součin ab, zobrazení $f : g \to (a,\ b)$ je tedy vzájemně jednoznačné. Je třeba ukázat, že „zobrazení zachovává operaci“, abychom ukázali, že se jedná o izomorfismus. Pro libovolné prvky $g_1 = a_1 b_1,\ g_2 = a_2 b_2$ platí:

$$f(g_1 g_2) = f(a_1 b_1 a_2 b_2) = f(a_1 a_2 b_1 b_2) = (a_1 a_2,\ b_1 b_2) ,$$
$$f(g_1) f(g_2) = f(a_1 b_1) f(a_2 b_2) = (a_1,\ b_1)(a_2,\ b_2) = (a_1 a_2,\ b_1 b_2) .$$

Vidíme, že $f(g_1 g_2) = f(g_1) f(g_2)$ a grupa G je tedy vskutku izomorfní direktnímu součinu podgrup $A,\ B$, což mělo být dokázáno.

Abelovy grupy

Abelovy grupy jsou speciálním případem grup, je na ně kromě základních tří axiomů kladen také požadavek na komutativitu grupové operace. Vlivem komutativity ztrácí některé z dříve definovaných pojmů informační hodnotu – například každá podgrupa komutativní grupy je normální, centrem grupy je celá grupa a rozkladem na vzájemně konjugované prvky získáme třídu jednoprvkových množin.

Na druhou stranu lze definovat celou řadu pojmů nových, jako lineární závislost/nezávislost či bázi grupy. Na jejich základě je možno exaktně popsat strukturu všech konečných (resp. konečně generovaných) Abelových grup. Ukazuje se, že pomocí již definovaného direktního součinu lze grupu rozložit na „atomické" části, podobně jako přirozená čísla rozkládáme v součin jejich základních stavebních prvků – prvočísel.

Lineární kombinací prvků $g_1, g_2, \dots, g_n$ rozumíme výraz

$$g_1^{e_1} g_2^{e_2} \dots g_n^{e_n} .$$

Řekneme, že množina $\{g_1, g_2, \dots, g_n\} \subseteq G$ je *lineárně nezávislá*, pokud platí

$$g_1^{e_1} g_2^{e_2} \dots g_n^{e_n} = 1 \Rightarrow \forall\, 1 \le i \le n;\ g_i^{e_i} = 1 .$$

Lineárně nezávislou množinu prvků grupy *G*, z níž lze lineární kombinací získat libovolný prvek grupy *G,* nazveme *bází* grupy *G*. Bázi grupy lze chápat jednak jako nejmenší možnou množinu generátorů grupy, jednak jako největší možnou lineárně nezávislou podmnožinu.

Je otázkou, jakým způsobem danou grupu rozkládat na části. Jako analogie prvočísel se nabízejí podgrupy, jejichž řád je prvočíslem. Již bylo ukázáno, že se jedná o grupy cyklické, tato analogie by však byla příliš omezující a nedokázali bychom popsat všechny komutativní grupy.

Další možností je utvořit podgrupy z prvků, jejichž řád (tj. řád podgrupy jimi generované) je roven danému prvočíslu. I tento koncept je ovšem příliš omezující.

S úspěchem lze použít teprve zobecnění předchozí množiny – množinu všech prvků, jejichž řád je libovolnou mocninou daného prvočísla *p.* (Přesně řečeno, při použití tohoto zobecnění nedostaneme atomické části, pro první náhled do struktury abelovských grup se však velmi dobře hodí.) Předně ukažme, že takto definovaná množina tvoří podgrupu *H* původní grupy *G* – neutrální prvek do této množiny patří, neboť triviální podgrupa je řádu 1, tedy p^0. Je-li dále $a \in H$, platí $a^{p^k} = 1$. Protože

$$(a^{-1})^{p^k} = (a^{p^k})^{-1} = 1 ,$$

obsahuje daná množina s každým prvkem i prvek inverzní. Konečně, předpokládejme, že $a, b \in H$, tedy

$$a^{p^k} = 1,\ b^{p^m} = 1 .$$

Označíme-li s větší z čísel *k, m*, platí jistě $(ab)^{p^s} = 1$, z čehož plyne závěr $ab \in H$. Tato podmnožina je tedy (spolu s indukovanou operací) podgrupou grupy *G*. Povšimněme si, že při důkazu příslušnosti součinu prvků *a, b* do grupy jsme mlčky předpokládali platnost komutativity, neboť pak

$$(ab)^{p^s} = a^{p^s} b^{p^s} = 1 .$$

Jak uvidíme dále, v případě grup neabelovských je situace odlišná, všechny prvky, jejichž řád je mocninou daného prvočísla, obecně podgrupu netvoří.

Dodejme ještě, že pokud prvočíslo *p* nedělí řád grupy, získáme (jak vyplývá z Lagrangeovy věty) triviální podgrupu.

Takto definovanou podgrupu grupy *G* nazveme *p-primární komponentou*, značíme $S(p)$. Jak posléze ukážeme, každou komutativní grupu řádu $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ lze rozložit v direktní součin jejích primárních komponent

$$S(p_1) \times S(p_2) \times \dots \times S(p_r) .$$

Prozatím je patrná pouze inkluze

$$S(p_1) \times S(p_2) \times \dots \times S(p_r) \subseteq G .$$

Fakt, že součin primárních komponent je direktní, plyne z nesoudělnosti prvočísel. K důkazu obrácené inkluze budeme potřebovat pomocné tvrzení (viz [6], str. 39):

Nechť je dána grupa G a její prvek a řádu mn, kde m, n jsou nesoudělná čísla. Pak lze tento prvek jednoznačně vyjádřit ve tvaru a = bc = cb, kde b je řádu m a c je řádu n. Prvky b, c jsou přitom mocninami prvku a.

Čísla jsou *m*, *n* nesoudělná, jejich největším společným dělitelem je tedy číslo 1. Z Euklidova algoritmu pro hledání největšího společného dělitele vyplývá, že existují celá čísla *u*, v taková, že

$$um + vn = 1 .$$

Potom ovšem zřejmě platí

$$a = a^1 = a^{um+vn} = a^{um} a^{vn} .$$

Označme $a^{um} = c$, $a^{vn} = b$ (na první pohled by bylo lepší označení obrácené, jak se však záhy ukáže, výhodnější je zvolit toto značení). Vidíme nyní, že $a = bc = cb$, nadto

$$b^m = a^{vnm} = a^{v(mn)} = e; \; c^n = a^{umn} = a^{u(mn)} = e .$$

Z posledních rovností vyplývá, že řád prvku *b* dělí číslo *m,* analogicky řád prvku *c* dělí *n,* označme tyto řády postupně m_1, n_1. Potom však

$$a^{m_1 n_1} = (bc)^{m_1 n_1} = b^{m_1 n_1} c^{m_1 n_1} = e .$$

To však znamená, že řád prvku *a*, který je dle předpokladů roven *mn*, dělí $m_1 n_1$, tedy

$$m_1 = m, \; n_1 = n .$$

Ukázali jsme tedy, že *b* je řádu *m* a *c* je řádu *n*. Zbývá ukázat jednoznačnost reprezentace.

Nechť tedy $a = bc = b_1 c_1$, kde prvky b, b_1 jsou řádu *m*, prvky c, c_1 jsou řádu *n*. Upravme rovnost na tvar

$$b_1^{-1} b = c_1 c^{-1} = w .$$

Z $b_1^{-1} b = w$ vyplývá $w^m = e$, z $c_1 c^{-1} = w$ vyplývá $w^n = e$. Protože jsou *m, n* nesoudělná, je nutně $w = e$, tedy $b = b_1$, $c = c_1$, což mělo být dokázáno.

Dodejme ještě, že předchozí větu lze zobecnit na nekomutativní grupy a také na případ, kdy řád prvku je součinem více vesměs nesoudělných čísel:

Nechť je dána grupa G a její prvek a řádu $n_1 n_2 \ldots n_r$, *kde* n_i *jsou vesměs nesoudělná čísla. Pak lze tento prvek jednoznačně vyjádřit ve tvaru* $a_1 a_2 \ldots a_r$, *kde* a_i *je řádu* n_i. *Prvky* a_i *jsou přitom mocninami prvku a.*

Nyní je čas vrátit se k rozkladu komutativních grup na direktní součin primárních komponent. Nechť je dána konečná komutativní grupa *G* a její libovolný prvek *a* řádu $p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$, kde p_i jsou navzájem různá prvočísla. Z předchozí věty plyne, že

$a = a_1 a_2 \ldots a_r$, přičemž a_i je řádu $p_i^{e_i}$.

Důsledkem toho $a_i \in S(p_i)$. S použitím předchozích výsledků dostáváme

$$S(p_1) \times S(p_2) \times \ldots \times S(p_r) = G .$$

Zjistili jsme tedy, že každá konečná komutativní grupa je direktním součinem svých primárních komponent. Prozkoumejme nyní, jakou mají tyto komponenty strukturu, pokusme se je tedy dále rozložit.

Nechť je dána *p*-primární komponenta $S(p)$ grupy *G*. Připomeňme, že všechny prvky podgrupy $S(p)$ mají řád rovný mocnině prvočísla *p*. Podívejme se nejprve na speciální případ, na cyklickou *p*-primární komponentu.

Chceme-li rozložit obecnou cyklickou grupu na direktní součin dvou jejích podgrup, je třeba nalézt normální podgrupy s triviálním průnikem, jejichž sjednocením je celá původní grupa. Jak víme, podgrupy cyklické grupy jsou rovněž cyklické, nadto pro každé číslo *m* dělící řád cyklické grupy *n* existuje právě jedna cyklická podgrupa řádu *m*. Konkrétně, je-li cyklická grupa složena z prvků

$$a , a^2 , \ldots , a^{n-2} , a^{n-1} ; n \in \mathbb{N} ,$$

pak pro každé *m*, kde *mk* = *n*, obsahuje podgrupa řádu *m* právě mocniny prvku a^k. Pro rozklad na direktní součin podgrup řádů *r, s* musí mít původní grupa řád *rs*. Pokud má být průnik těchto dvou podgrup triviální, je zřejmě nutné, aby nejmenší společný násobek čísel *r*, *s* byl roven *rs*, to ovšem nastane právě tehdy, jsou-li *r, s* nesoudělná. Ukázali jsme tedy, že pokud lze obecnou cyklickou grupu rozložit na direktní součin dvou jejích podgrup, jsou řády těchto podgrup navzájem nesoudělné.

Vrátíme-li se nyní k cyklickým primárním komponentám, zjišťujeme následující – řády všech netriviálních podgrup jsou mocninou daného prvočísla, tedy jsou tímto prvočíslem dělitelné, tedy jsou soudělné. Cyklická primární komponenta je tudíž nerozložitelná, tzv. *direktně ireducibilní*.

Zbývá prozkoumat případ necyklických primárních komponent. Řády všech prvků *p*-primární komponenty $S(p)$ jsou rovny mocnině daného prvočísla *p*. Zvolme jeden z prvků maximálního řádu, grupu jím generovanou označme *H*. Dále nalezněme maximální podgrupu *K* grupy $S(p)$ takovou, že

$$H \cap K = \{e\} .$$

Grupa $S(p)$ je direktním součinem těchto podgrup, tedy

$$S(p) = H \times K .$$

Důkaz tohoto tvrzení lze nalézt např. v [5], str. 133–134.

Necyklickou primární komponentu lze tedy rozložit v direktní součin dvou podgrup ostře menších řádů, přičemž minimálně jedna z těchto podgrup bude cyklická. Opakováním tohoto postupu lze každou primární komponentu vyjádřit jako direktní součin cyklických podgrup.

Jelikož řád každé z těchto cyklických grup je mocninou prvočísla *p*, je díky definici direktního součinu i řád primární komponenty roven mocnině prvočísla *p*.

Nechť je dána grupa *G* řádu

$$n = p_1^{e_1} p_2^{e_2} \dots p_i^{e_i};\ i \in \mathbb{N}\ .$$

Ukázali jsme již, že tuto grupu lze rozložit na direktní součin jejích primárních komponent. Vzhledem k výsledkům z předchozího odstavce se jedná právě o ty podgrupy, které odpovídají prvočíslům nacházejícím se v rozkladu čísla *n*. Činitele p_j ve faktorizaci čísla *n* lze získat pouze jako dělitele řádu odpovídající primární komponenty $S(p_j)$, tedy primární komponenta $S(p_j)$ je řádu $p_j^{e_j}$. Sama je direktním součinem cyklických podgrup řádů

$$p_j^{e_{j_1}},\ \ p_j^{e_{j_2}},\ \ \dots\ , p_j^{e_{j_k}},$$

přičemž platí

$$e_{j_1} + e_{j_2} + \dots + e_{j_k} = e_j\ .$$

Z definice direktního součinu vyplývá, že jsou-li zadány řády cyklických podgrup

$$p_j^{e_{j_1}},\ p_j^{e_{j_2}},\ \dots\ ,\ p_j^{e_{j_k}},$$

je tím (až na izomorfismus) určena odpovídající primární komponenta $S(p_j)$. Daným řádům říkáme invarianty podgrupy $S(p_j)$. Někdy hovoříme též o invariantech grupy, čímž máme na mysli řády cyklických podgrup z rozkladu celé grupy.

Platí však i obrácené tvrzení – pokud danou primární komponentu rozložíme v direktní součin cyklických podgrup, získáme vždy stejný počet činitelů, navíc řády podgrup budou stejné, samozřejmě až na pořadí (viz např. [6], str. 41).

Vidíme, že komutativní grupa je (až na izomorfismus) určena svými invarianty. Můžeme tedy již přistoupit ke klasifikaci Abelových grup do řádu patnáct, pro přehlednost vynechejme již klasifikované grupy prvočíselného řádu:

Řád	Grupy
4	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$
6	$\mathbb{Z}_2 \times \mathbb{Z}_3$
8	$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
9	$\mathbb{Z}_9,\ \mathbb{Z}_3 \times \mathbb{Z}_3$
10	$\mathbb{Z}_2 \times \mathbb{Z}_5$
12	$\mathbb{Z}_3 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$
14	$\mathbb{Z}_2 \times \mathbb{Z}_7$
15	$\mathbb{Z}_3 \times \mathbb{Z}_5$

Jelikož cyklické grupy jsou, jak jsme již dříve ukázali, komutativní, musí platit rovnosti

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_6,\ \mathbb{Z}_2 \times \mathbb{Z}_5 = \mathbb{Z}_{10},\ \mathbb{Z}_2 \times \mathbb{Z}_7 = \mathbb{Z}_{14}\ .$$

Nabízí se hypotéza, že pro navzájem různá prvočísla *p, q* platí

$$\mathbb{Z}_p \times \mathbb{Z}_q = \mathbb{Z}_{pq}\ .$$

Vskutku, nechť jsou dány prvky $a \in \mathbb{Z}_p,\ b \in \mathbb{Z}_q$. Platí tedy

$$a^p = e\ ,\ b^q = e\ .$$

Označme $c = ab$, pak zřejmě $c^{pq} = e$, ukažme dále, že číslo *pq* je navíc vhledem k této

vlastnosti minimální. Protože mocniny prvku c tvoří cyklickou podgrupu, přichází v úvahu pouze čísla p nebo q. Kdyby ovšem platilo $c^p = e$, pak bychom dále získali

$$e = c^p = (ab)^p = a^p b^p = e\, b^p = b^p .$$

To je ovšem spor s předpokladem $b^q = e$. Analogicky se vyvrátí i druhá možnost.

Ukázali jsme tedy, že grupa, jejímiž invarianty jsou dvě vzájemně různá prvočísla, je cyklická. Tvrzení se snadno rozšíří i na libovolný konečný počet vesměs různých prvočíselných invariantů.

Zbývá otázka, která z grup řádu 12 je cyklická, díky tomu, že nejmenším společným násobkem čísel 3 a 4 je 12 je to grupa $\mathbb{Z}_3 \times \mathbb{Z}_4$.

Sylowovy podgrupy

Připomeňme na tomto místě myšlenku primárních komponent, jak jsme ji zavedli v oddíle o komutativních grupách – zde *všechny* prvky, jejichž řád byl mocninou daného prvočísla *p*, tvořily grupu, tuto grupu jsme nazvali *p*-primární komponentou a označili jsme ji $S(p)$. Při důkazu jsme ovšem využili komutativity, tudíž nelze předpokládat, že i v případě obecné grupy budou všechny prvky splňující danou podmínku tvořit grupu. Koncept primárních komponent tedy budeme muset zobecnit.

P-podgrupou (obecně i p-grupou) rozumíme podgrupu (resp. grupu), jejíž každý prvek má řád rovný nějaké mocnině prvočísla p. Sylowovou p-podgrupou dané grupy G rozumíme maximální p-podgrupu dané grupy G.

Všimněme si, že Sylowova *p*-podgrupa existuje pro každou konečnou grupu *G a* pro libovolné prvočíslo *p*, neboť přinejmenším triviální podgrupa je *p*-podgrupou. Pokud se podíváme na definici *p*-primární komponenty u komutativních grup, zjistíme, že i *p*-primární komponenta je vlastně Sylowovou *p*-podgrupou, neboť tvoří-li množina *všech* prvků řádu p^n podgrupu, je tato podgrupa zřejmě Sylowovou (maximální) *p*-podgrupou. Proto někteří autoři používají pojem Sylowova podgrupa i v případě Abelových grup.

Na rozdíl od případu komutativních grup může obecně existovat více maximálních *p*-podgrup dané grupy *G*. Řády Sylowových podgrup popisuje první Sylowova věta, o jejich struktuře, resp. počtu vypovídají druhá, resp. třetí Sylowova věta.

Sylowovy věty

V této části uvedeme tři základní věty, které jsou důležité pro studium stavby grup. Jedná se o tzv. *Sylowovy věty*.

Jak jsme již zdůraznili v pasáži o Lagrangeově větě, fakt, že číslo *m* dělí řád grupy *G*, ještě nezaručuje existenci podgrupy řádu *m*. Ukazuje se ovšem, že omezíme-li se na *prvočíslo p* (případně na jeho mocninu p^k) dělící řád grupy *G*, existence podgrupy řádu *p* (resp. p^k) je zaručena. Můžeme tedy vyslovit následující velmi důležité tvrzení, zvané 1. Sylowova věta:

Nechť je dáno prvočíslo p a nechť jeho mocnina p^k; $k \in \mathbb{N}$ *dělí řád grupy G. Potom grupa G obsahuje podgrupu řádu* p^k.

Důkaz proveďme indukcí dle řádu grupy *G*, označme jej *n*, využijeme zejména Lagrangeovy věty a třídové rovnice. Rozdělíme jej do dvou větví v závislosti na tom, zda *p* dělí řád centra grupy.

Připomeňme, že centrem grupy *G* rozumíme množinu

$$C(G) = \{a \in G;\ \forall g \in G:\ g^a = g\}\ .$$

Platí tedy $\forall x,\ y \in C(G):\ y^{-1} x\, y = x$, po úpravě $xy = yx$. Vidíme, že prvky centra komutují, neboli centrum je nejen grupou, ale dokonce Abelovskou grupou. Nadto ukažme, že centrum je i normální podgrupou původní grupy – pro centrum grupy platí

$$\forall x \in G\ \forall a \in C(G):\ x^a = x\text{, tedy }\ \forall x \in G\ \forall a \in C(G):\ a^{-1} x a = x\ .$$

Poslední rovnost lze přepsat do tvaru

$$\forall x \in G\, \forall a \in C(G):\ a = x^{-1} a\, x\text{, což není nic jiného než }\ \forall x \in G\, \forall a \in C(G):\ a^x = a\ .$$

Vidíme, že prvky centra se po transformaci libovolným prvkem zobrazí na sebe, což je podmínka „silnější“, než zobrazení normální podgrupy na sebe. Ukázali jsme, že centrum je normální abelovskou podgrupou původní grupy.

Pro $n = 1$ je platnost výroku zřejmá, předpokládejme tedy, že $n > 1$.

Nechť nejprve prvočíslo *p* dělí řád centra $C(G)$ grupy *G*. Protože je dle právě dokázaného centrum abelovskou grupou, nutně obsahuje (jak je ukázáno v pasáži o komutativních grupách) cyklickou podgrupu řádu *p*, označme ji P. Snadno se ukáže, že podgrupa centra je rovněž normální podgrupou grupy původní, můžeme tedy vytvořit faktorovou grupu původní grupy dle této cyklické podgrupy. Tato grupa – označme ji *G/P* – je řádu *n/p*. Předpokládali jsme, že řád původní grupy je dělitelný p^k, řád faktorové grupy je proto dělitelný číslem p^{k-1}. Protože je faktorová grupa ostře menšího řádu než grupa původní (řád centra je dělitelný prvočíslem, je tedy větší než jedna), s využitím indukčního kroku lze tvrdit, že faktorová grupa obsahuje podgrupu řádu p^{k-1}. V původní grupě *G* ovšem této podgrupě odpovídá podgrupa řádu $p^{k-1} p = p^k$, což mělo být dokázáno.

Pokud prvočíslo *p* řád centra grupy *c* nedělí, postupujme následovně – pomocí třídové rovnice lze řád grupy *G* vyjádřit ve tvaru

$$|G| = c + x_1 + x_2 + \ldots + x_q;\ q \in \mathbb{N}\ ,$$

kde *c* je řád centra.

Z toho, že p nedělí c plyne, že p nemůže dělit všechny sčítance x_i; $1 \le i \le q$, neboť by se pravá strana rovnice dala přepsat do tvaru

$$c + pn;\ n \in N,\ p \nmid c.$$

Bez újmy na obecnosti předpokládejme, že p nedělí x_1. Jak jsme ovšem dříve ukázali, číslo x_1 odpovídá indexu jisté podgrupy H (konkrétně normalizátoru některého z prvků dané třídy ekvivalence), jejíž řád označíme h. Zbytek důkazu je triviální – protože $n = x_1 h$ a $p \nmid x_1,\ p^k \mid n$, musí platit, že $p^k \mid h$. Dle předpokladů tedy grupa H (a s ní i původní grupa G) obsahuje podgrupu řádu p^k, čímž je důkaz hotov (viz [9], str. 158–159).

O vzájemném vztahu Sylowových podgrup vypovídá druhá Sylowova věta (viz [6], str. 45–46):

Všechny Sylowovy p-podgrupy dané konečné grupy jsou vzájemně konjugované, tudíž izomorfní.

Dříve než začneme s důkazem druhé Sylowovy věty, zavedeme nejprve pojem třídy grupy podle dvou jejích podgrup. Připomeňme teorii tříd grupy podle jedné její podgrupy. Nechť je dána grupa G *a* její podgrupa H. Levou třídou grupy G podle podle podgrupy H rozumíme libovolnou množinu tvaru

$$aH = \{ah : h \in H\}\text{, kde } a \in G \text{ je pevně zvolený prvek.}$$

Ukázali jsme, že každé dvě takto utvořené třídy jsou buď totožné nebo disjunktní, nadto mají všechny tyto třídy stejný počet prvků jako podgrupa H. Z toho již vyplývá, že počet vzájemně různých tříd je roven číslu $|G|:|H|$ (a tedy počet prvků podgrupy H nutně dělí počet prvků grupy G, jak tvrdí Lagrangeova věta).

Mějme nyní dány dvě podgrupy H, K grupy G *a* utvořme třídy tvaru

$$HaK = \{hak : h \in H,\ k \in K\}\text{, kde } a \in G \text{ je pevně zvolený prvek.}$$

Opět platí, že každé dvě takto utvořené třídy jsou totožné nebo disjunktní – předpokládejme, že třídy $HaK,\ HbK$ nejsou disjunktní, tedy

$$\exists g \in G : g = h_1 a k_1 = h_2 b k_2.$$

Potom však libovolný prvek ze třídy HaK lze přepsat jako

$$hak = h(h_1^{-1}h_1)a(k_1k_1^{-1})k = hh_1^{-1}(h_1 a k_1)k_1^{-1}k = hh_1^{-1}(h_2 b k_2)k_1^{-1}k = (hh_1^{-1}h_2)b(k_2k_1^{-1}k).$$

Vzhledem k tomu, že platí

$$hh_1^{-1} \in H,\ k_2k_1^{-1}k \in K$$

jsme právě ukázali inkluzi $HaK \subseteq HbK$, opačná inkluze se ukáže analogicky.

Třída HaK zřejmě obsahuje ty *pravé* třídy grupy G podle podgrupy H, které lze vyjádřit ve tvaru

$$Hak,\ k \in K.$$

Stejně tak obsahuje ty *levé* třídy (grupy G) podle podgrupy K, které lze vyjádřit jako

$$haK,\ h \in H.$$

Počty těchto pravých, resp. levých tříd ukazuje následující věta.

Nechť je dána grupa G a dvě její podgrupy H, K a nechť x je libovolný pevně zvolený prvek grupy G. Pak počet pravých tříd grupy G podle podgrupy H, resp. počet levých tříd grupy G podle podgrupy K, obsažených ve třídě HxK je roven

$$[K : K \cap x^{-1} Hx] \text{, resp. } [x^{-1} Hx : K \cap x^{-1} Hx] .$$

Důkaz této věty lze nalézt např. v [6], str. 15.

Přistupme nyní již k důkazu druhé Sylowovy věty.

Nechť P_1, P_2 jsou dvě Sylowovy *p*-podgrupy grupy *G*. Rozložíme grupu *G* na třídy podle těchto dvou podgrup, tedy

$$G = P_1 x_1 P_2 + P_1 x_2 P_2 + \ldots + P_1 x_s P_2 .$$

Označme b_i počet levých tříd grupy *G* podle podgrupy P_2, které jsou obsaženy ve třídě

$$P_1 x_i P_2 .$$

Podle předchozí věty platí

$$b_i = [x_i^{-1} P_1 x_i : x_i^{-1} P_1 x_i \cap P_2] .$$

Jelikož konjugovaná podgrupa $P_1^{x_i}$ má stejný počet prvků jako původní podgrupa P_1 a průnik podgrup je opět podgrupou, musí být (s přihlédnutím k tomu, že P_1, P_2 jsou Sylowovy *p*-podgrupy) $b_i = 1$, resp. $b_i = p^n ; n \in \mathbb{N}$.

Vzhledem k faktu, že třídy $P_1 x_i P_2$ tvoří rozklad, je

$$b_1 + b_2 + \ldots + b_s = [G : P_2] .$$

Protože je podgrupa P_2 Sylowova, tedy maximální *p*-podgrupa, nutně platí $p \nmid [G : P_2]$. V důsledku toho tedy pro některý ze sčítanců z poslední rovnosti platí $b_i = 1$. To však znamená, že

$$P_1^{x_i} = P_2 \text{, což mělo být dokázáno.}$$

Jak již bylo řečeno, třetí Sylowova věta vypovídá o počtu Sylowových *p*-podgrup dané grupy:

Počet Sylowových p-podgrup dané konečné grupy G dělí její řád a nadto jej lze vyjádřit ve tvaru $kp + 1, k \in \mathbb{N}_0$.

Tvrzení je zřejmé pro případ jedné podgrupy, předpokládejme tedy, že $S_0, S_1, \ldots, S_r$ jsou všechny Sylowovy *p*-podgrupy dané grupy G $(r \geq 1)$. Již víme, že každé dvě z těchto podgrup jsou konjugované, tedy

$$\forall\, 0 \leq i \leq r \;\forall\, 0 \leq j \leq r \;\exists g \in G : S_i^g = S_j .$$

Omezíme-li se ovšem pouze na „konjugující“ prvky z množiny S_0, zřejmě již nemusí platit, že každé dvě grupy jsou konjugované. Díky tomu, že S_0 je podgrupa, bude i takto omezená konjugovanost ekvivalencí, tedy třída Sylowových *p*-podgrup

$$S_0, S_1, \ldots, S_r$$

se rozloží na třídy Sylowových podgrup vzájemně konjugovaných prvky z S_0. Uvažujme nyní normalizátor K_i grupy S_i. Předně tento normalizátor obsahuje grupu S_i, navíc platí $S_i \lhd K_i$. Ukažme, že S_i je jediná Sylowova p-podgrupa obsažená v normalizátoru K_i (viz [W8]). Vskutku, nechť navíc $S_j \subseteq K_i$, $i \neq j$. Pak jsou obě podgrupy S_i, S_j Sylowovými

p-podgrupami v grupě K_i(!). Podle druhé Sylowovy věty jsou tyto podgrupy konjugované v K_i, tedy

$$S_i^k = S_j,\ k \in K_i .$$

Podgrupa S_i je však normální podgrupou svého normalizátoru K_i, tedy

$$\forall\, k \in K_i \colon S_i^k = S_i .$$

Získáváme tedy $i = j$, což je spor. Normalizátor K_i obsahuje tedy jedinou Sylowovu p-podgrupu, podgrupu S_i. Tedy

$$K_i \cap S_0 \subset S_0,\ i \neq 0$$

(všimněte si ostré inkluze). Index normalizátoru K_i v grupě S_0 je tedy větší než jedna, tedy je roven mocnině prvočísla p. Tomuto indexu však odpovídá i počet podgrup konjugovaných s podgrupou S_i při použití „konjugujících“ prvků z grupy S_0. Celkový počet podgrup lze pomocí tohoto rozkladu na třídy zapsat ve tvaru

$$1 + p^{e_1} + p^{e_2} + \ldots + p^{e_t},\ e_i > 0 .$$

Tento výraz lze přepsat do tvaru

$$1 + p(p^{e_1 - 1} + p^{e_2 - 1} + \ldots + p^{e_t - 1}) = 1 + kp .$$

Zbývá ukázat, že počet Sylowových p-podgrup dělí řád grupy G. To však plyne ihned z rovnosti tohoto počtu a indexu normalizátoru podgrupy S_0.

Struktura grup řádů p^2, pq, $2p$, 8 a 12

1 Grupy řádu p^2

Než začneme se studiem grup, jejichž řád je druhou mocninou prvočísla, ukažme nejprve platnost jedné důležité pomocné věty:

Centrum libovolné konečné p-grupy je netriviální.

Nechť je dána konečná *p*-grupa G. Počet jejích prvků lze dle třídové rovnice vyjádřit ve tvaru

$$p^m = 1 + x_1 + x_2 + \ldots + x_r;\ r \in \mathbb{N},$$

kde sčítance odpovídají třídám vzájemně konjugovaných prvků (číslo jedna reprezentuje neutrální prvek, který je konjugován pouze sám se sebou). Jak víme, mohutnosti tříd jsou rovny indexům jistých normalizátorů, tedy dělí řád grupy. Všechny sčítance musí být tudíž rovny mocnině *p*, případně jedné. Kdyby ovšem každé x_i bylo mocninou *p*, pravá strana třídové rovnice by nebyla dělitelná *p*, což je spor. Nutně tedy existuje prvek různý od neutrálního, konjugovaný pouze sám se sebou. Centrum grupy obsahuje i tento prvek, není proto triviální.

Dále ukážeme, že grupa řádu p^2 je nutně Abelovská.

Připomeňme definici normalizátoru prvku *x* grupy *G*:

$$N(x) = \{a \in G;\ x^a = x\}.$$

Rovnost $x^a = x$ lze přepsat do tvaru $xa = ax$, z něj je zřejmé, že normalizátorem prvku rozumíme množinu prvků, které s tímto prvkem komutují. Protože centrum je množina prvků, které komutují se *všemi* prvky grupy, zřejmě $C(G) \subseteq N(x)$. Navíc jistě i $x \in N(x)$. Je-li *x* prvkem centra grupy, znamená to, že komutuje se všemi prvky grupy, a tedy $N(x) = G$. Není-li *x* prvkem centra grupy, pak z předchozího vyplývá $|C(G)| < |N(x)|$. Centrum grupy je ovšem netriviální, tedy jeho mohutnost je minimálně *p*. Pak ovšem $|N(x)| = p^2$, čili opět $N(x) = G$. Ukázali jsme, že každý prvek dané grupy komutuje se všemi prvky grupy, což mělo být dokázáno.

Cílem práce je popis grup do řádu patnáct, této kapitoly se tedy týkají pouze řády čtyři a devět.

U grupy řádu čtyři připadají v úvahu invarianty 4, resp. 2, 2. Jim odpovídají cyklická grupa $\mathbb{Z}_4$, resp. direktní součet cyklických grup $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Analogicky získáme v případě devíti prvků možnosti $\mathbb{Z}_9$, resp. $\mathbb{Z}_3 \times \mathbb{Z}_3$.

2 Grupy řádu pq

Do tohoto oddílu spadají grupy řádů 6, 10, 14 a 15, postupujme však obecně.

Nechť je tedy dána grupa *G* řádu $pq;\ p > q$ (*p, q* jsou prvočísla). Dle třetí Sylowovy věty dělí počet Sylowových *p*-podgrup číslo *pq*, navíc jej lze vyjádřit ve tvaru $n = kp + 1$. Počet těchto podgrup nemůže být roven *p* ani *pq,* neboť $p \nmid kp + 1$. Protože $p > q$, zřejmě nemůže být počet podgrup roven ani prvočíslu *q*. Grupa *G* tedy obsahuje pouze jednu Sylowovu *p*-podgrupu, která je tudíž normální (neboť je konjugovaná pouze sama se sebou). Počet Sylowových *q*-podgrup opět dělí *pq*, nadto je tvaru $kq + 1$. Analogicky jako v předchozím případě můžeme vyloučit počty *pq*, *q*.

Pokud je i počet Sylowových q-podgrup roven jedné, obsahuje grupa G dvě normální podgrupy s triviálním průnikem. Jelikož sjednocením těchto grup je celá grupa G, platí $G = S(p) \times S(q)$. Označme generátory direktních sčítanců po řadě a, b.

Zřejmě $a^p = b^q = e$. Označíme-li $c = ab$, vidíme, že

$$c^{pq} = (ab)^{pq} = a^{pq} b^{pq} = (a^p)^q (b^q)^p = e .$$

Kdyby platilo $c^q = e$, muselo by nutně platit $e = (ab)^q = a^q b^q = a^q$, což je spor, neboť a generuje grupu řádu p, $p > q$. Neplatí ovšem ani $c^p = e$. V tom případě by totiž platilo

$$e = (ab)^p = a^p b^p = b^p .$$

Zvolíme-li nyní číslo r tak, že $p = kq + r,\ k \in \mathbb{Z},\ r \in \mathbb{Z},\ r > 0$ (zbytek po celočíselném dělení), získáváme rovnost $b^r = e$, což je opět spor (vzhledem k nerovnosti $r < q$).

Prvek c je tedy řádu pq, z čehož vyplývá, že generuje grupu G, která je proto cyklická (tedy komutativní).

Opomněli jsme zatím možnost $kq + 1 = p$, která může nastat u grup řádu 6, 10 a 14. Tuto možnost však probereme v následující části.

Hlavním výsledkem tohoto oddílu je tvrzení, že grupa řádu pq, kde $p > q$ a $q \nmid p - 1$, je cyklická.

3 Grupy řádu 2*p*

Popišme dále strukturu grup řádu $2p$, kde p je prvočíslo větší než 2.

Nechť je dána grupa G řádu $2p$. Pokud existuje prvek řádu $2p$, jedná se o cyklickou grupu.

Předpokládejme, že žádný z prvků není řádu $2p$. Z první Sylowovy věty vyplývá, že existuje podgrupa řádu p. Ta je zřejmě cyklická, analogicky jako v předchozí části se ukáže, že je normální; označme generátor této podgrupy a a podgrupu samotnou H.

Zvolme nyní prvek $b \notin H$. Z pasáže o třídách grupy vyplývá, že množiny H a bH jsou disjunktní, navíc

$$G = H \cup bH .$$

Ukažme, že $b^2 = e$: kdyby platilo $b^2 \in bH$, získali bychom jednoduchou úpravou $b \in H$, což je spor s volbou b. Pokud by dále platila rovnost

$$b^2 = a^i,\ 1 < i < p ,$$

pak, s přihlédnutím k tomu, že prvek a^i je řádu p, by řád prvku b byl roven $2p$, což je spor s acykličností grupy.

Zatím jsme tedy získali množinu

$$\{e, a, a^2, \ldots, a^{p-1}, b, ba, \ldots, ba^{p-1}\} .$$

Pokud pro množinu Hb provedeme analogickou úvahu jako pro bH, získáme rovnost

$$Hb = bH ,$$

což znamená, že $ab = ba^i$. Tedy

$$a = ae = ab^2 = (ab)b = ba^i b = ba^{i-1}(ab) = ba^{i-1} ba^i = \ldots = a^{i^2} .$$

Z právě obdržené rovnosti vyplývá $a^{i^2-1} = e$ a dále také $p \mid i^2 - 1$. Pro i dostáváme dvě možnosti, $i = kp + 1$ a $i = kp - 1$.

V prvním případě musí platit $ab = ba$, $(ab)^p = b^p = b$ (neboť p je liché), tedy ab je řádu $2p$ a generuje celou grupu, která je tudíž cyklická.

Z druhého případu získáváme rovnost $ab = ba^{-1}$. Tím je již jednoznačně definována grupová operace.

Není obtížné si představit cyklickou grupu řádu $2p$ – zvolíme-li např. $p = 3$, lze jako příklad použít grupu všech zákrytových rotací pravidelného šestiúhelníku, případně grupu $\mathbb{Z}_6$. Ale co druhý případ?

Pokud se zamyslíme nad naznačenou strukturou hledané grupy, pak zjistíme, že obsahuje v podstatě p „otočení“ (prvky $e, a, \ldots, a^{p-1}$) a p „otočení transformovaných prvkem b“. Navíc tento prvek b dává při umocnění prvek neutrální. Ovšem přesně takto lze nahlížet (stále platí $p = 3$) na grupu zákrytových pohybů rovnostranného trojúhelníku (zmiňovanou v úvodu)! Prohlašme libovolnou z osových symetrií trojúhelníku za prvek b, pak lze veškeré zákrytové pohyby popsat takto – jedná se buď o otočení, čili pohyb, při kterém se nemění orientace vrcholů, nebo o osovou symetrii složenou s otočením, čili nepřímý zákrytový pohyb. Platnost $ab = ba^{-1}$ plyne z vlastností osové symetrie, která „mění orientaci úhlů“ (jak je trefně uvedeno v [W5], rovnost $b^{-1}ab = a^{-1}$ vyjadřuje, že rotace v zrcadle vypadá jako rotace inverzní).

Jelikož osovou symetrii složenou s otočením lze nahradit vhodnou (jinou) symetrií, lze se na tuto grupu dívat jako na grupu tří otočení a tří osových symetrií. Obecně pro libovolné $p \geq 3$ můžeme takto vytvořit grupu symetrií pravidelného p-úhelníku, která bude obsahovat p otočení a p osových symetrií, tedy celkem $2p$ prvků.

Snadno nahlédneme, že stejnou grupu zákrytových pohybů má i jistý dvojjehlan (tedy těleso, které vznikne „slepením“ dvou shodných pravidelných p-bokých jehlanů podstavami k sobě). Pokud budeme rovnostranný trojúhelník chápat jako degenerovaný případ trojrozměrného tělesa s nulovou výškou, lze jej považovat za jakýsi „dvojstěn“ – diedr. Proto se tato grupa často nazývá grupa diedrická či dihedrální, značíme D_p, resp. D_{2p} dle toho, zda chceme spíše postihnout počet prvků grupy či počet stran „diedru“. Navíc zákrytový pohyb odpovídající osové symetrii nelze v rovině provést, proto tímto názvem vlastně ospravedlňujeme použití osových symetrií. V této práci se nadále budeme držet druhého typu značení (neboť klademe větší důraz na algebraický charakter, nikoliv na charakter geometrický).

Nyní nám ke klasifikaci zbývají grupy řádů 8 a 12. Protože obecné úvahy na téma grup řádů p^3, resp. pqr by byly zbytečně komplikované, zaměříme se rovnou na tyto řády.

4 Grupy řádu 8

Všechny Abelovské grupy řádu 8 jsou, jak jsme již ukázali, izomorfní s jednou z grup

$$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

zaměřme se proto pouze na grupy neabelovské.

Při klasifikaci využijeme následující pomocné věty:

Pokud je řád všech prvků grupy kromě neutrálního roven dvěma, je grupa abelovská.

Je-li řád grupy roven dvěma, jedná se o cyklickou grupu $\mathbb{Z}_2$, která je zřejmě abelovská.

V opačném případě zvolme prvky $a, b \in G$ různé od prvku neutrálního. Tedy

$$a^2 = b^2 = e \text{, dále } a = a^{-1},\ b = b^{-1}.$$

Z rovností

$$(ab)^2 = (ab)(ab) = a(ba)b\ ,\ ba = a^{-1}b^{-1} = ab$$

již vyplývá dokazovaná komutativita.

Nyní se již vraťme k našemu problému – klasifikaci nekomutativních grup řádu 8.

V důsledku Lagrangeovy věty mají ve zkoumaných grupách všechny prvky kromě neutrálního řád 2, 4 či 8. Právě jsme ukázali, že případ, kdy mají všechny prvky řád 2 můžeme vyloučit. Jelikož prvek řádu 8 by znamenal, že grupa je cyklická, tudíž komutativní, grupa musí nutně obsahovat prvek řádu 4, označme jej *a*. Označme dále *b* jeden z prvků negenerovaných prvkem *b*. Prvky

$$\{e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b\}$$

jsou při splnění požadavků na prvky *a, b* vzájemně různé. Mocnina prvku *b* musí být rovna některému z prvků $e,\ a,\ a^2,\ a^3$, jinak bychom po vykrácení prvkem *b* ukázali, že je tento prvek generován prvkem *a*. Pokud by dále platilo

$$b^2 = a \text{, resp. } b^2 = a^3,$$

řád prvku *h* by byl roven 8, což je spor. Zbývají tudíž možnosti

$$b^2 = e \text{, resp. } b^2 = a^2.$$

V prvním případě zjistíme, že *ba* je rovno jednomu z prvků $ab,\ a^2b,\ a^3b$. Přitom první možnost dává komutativní grupu. Z druhé možnosti postupně vyplývá

$$ba = a^2b\ ,\ b^{-1}a^2b = a\ ,\ (b^{-1}a^2b)^2 = (b^{-1}a^2b)(b^{-1}a^2b) = b^{-1}a^4b = e,\ a^2 = e\ ,$$

což je spor, neboť prvek *a* je řádu 4. Jedinou možností je tedy $ba = a^3b$, z čehož dále získáváme

$$ba = a^{-1}b,\ aba = b\ ,\ ab = ba^{-1}.$$

Násobení je tedy definováno rovnostmi $a^4 = b^2 = e,\ ab = ba^{-1}$. V předchozí části jsme již ukázali, že se jedná o dihedrální grupu D_8, tedy grupu zákrytových pohybů pravidelného čtyřbokého dvojjehlanu (resp. čtverce).

Analogicky jako v prvním případě se i v případě druhém ukáže $ba = a^3b$. Jelikož je toto poslední zbývající grupa řádu 8, pak (s přihlédnutím k tomu, že grupa kvaternionů je nekomutativní a neizomorfní s D_8) se zřejmě jedná o grupu kvaternionů – lze zvolit např. značení

$$a = i,\ b = j \text{, pak dostáváme prvky}$$

$$e = 1,\ \ i,\ \ i^2 = -1,\ \ i^3 = -i,\ \ \ j,\ \ ij = k,\ \ i^2j = -j,\ \ i^3j = -k.$$

Grupu kvaternionů značíme Q.

Ukázali jsme, že každá grupa řádu 8 je izomorfní s některou z grup

$$\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ D_8,\ Q.$$

5 Grupy řádu 12

Dříve než začneme s klasifikací grupy řádu 12, vraťme se ještě k popisu grupy kvaternionů. Vycházeli jsme z množiny prvků

$$\{e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b\},$$

přičemž dále platilo $b^2 = a^2,\ ba = a^{-1}b$. Nabízí se následující zobecnění:

Vezměme množinu

$$\{e,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ b,\ ab,\ a^2b,\ a^3b,\ a^4,\ a^5b\}$$

a analogicky jako u kvaternionů definujme $b^2 = a^3,\ ba = a^{-1}b$.

Obecněji lze pro libovolné $n \in \mathbb{N}$ definovat grupu jako množinu

$$\{e,\ a,\ a^2,\ \ldots,\ a^{2n-1},\ b,\ ab,\ a^2b,\ \ldots,\ a^{2n-1}b\}$$

spolu s násobením $b^2 = a^n,\ ba = a^{-1}b$.

Lze ukázat, že tato struktura je skutečně grupou, značíme ji Dic_n a nazýváme dicyklickou grupou. Řád grupy Dic_n je zřejmě 4*n*, dále $Q = Dic_2$.

S přihlédnutím k dříve ukázanému vidíme, že existují přinejmenším následující grupy řádu 12 – komutativní $\mathbb{Z}_3 \times \mathbb{Z}_4 = \mathbb{Z}_{12},\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ a nekomutativní $D_{12},\ A_4,\ Dic_3$. Jelikož řády prvků grup $D_{12},\ A_4,\ Dic_3$ jsou po řadě 1, 2, 2, 2, 2, 2, 2, 2, 3, 3, 6, 6; 1, 2, 2, 2, 3, 3, 3, 3, 3, 3, 3, 3; 1, 2, 3, 3, 4, 4, 4, 4, 4, 4, 6, 6; nejsou žádné dvě z těchto grup izomorfní. Dále ukážeme, že každá grupa řádu 12 je izomorfní s jednou z grup právě zmíněných, tj. existuje právě pět grup řádu 12 (viz [W6]).

Předpokládejme, že *G* je neabelovská grupa řádu 12. Označme s_2, resp. s_3 počet Sylowových 2-podgrup, resp. 3-podgrup. Ze třetí Sylowovy věty vyplývá

$$s_2 | 12,\ s_2 \equiv 1\ (mod\ 2),$$

těmto podmínkám vyhovují $s_2 = 1,\ s_2 = 3$. Analogicky podmínkám

$$s_3 | 12,\ s_3 \equiv 1\ (mod\ 3)$$

vyhovují $s_3 = 1,\ s_3 = 4$. Probereme nyní postupně všechny čtyři možné kombinace:

1. $s_2 = 1,\ s_3 = 1$: V tomto případě jsou obě Sylowovy podgrupy normální, navíc jejich průnik je triviální a sjednocením je původní grupa, tedy $G = S(2) \times S(3)$. Všimněme si dále následujícího – grupa $S(2)$ je řádu 4, grupa $S(3)$ je řádu 3, jak jsme již ukázali, jsou všechny grupy těchto řádů komutativní, a tedy je komutativní i direktní součin těchto grup. To je ovšem spor s volbou původní grupy.
2. $s_2 = 3,\ s_3 = 4$: Také pro tuto možnost odvodíme spor – výsledná grupa by obsahovala 8 prvků řádu 3, neutrální prvek a minimálně 4 prvky, jejichž řád je mocninou čísla 2, tedy celkem minimálně 13 prvků.
3. $s_2 = 1,\ s_3 = 4$: Pro tato čísla získáváme následující fakta – grupa *G* obsahuje normální podgrupu řádu 4 (označme ji *K*) a další podgrupu *H* (která není normální). Navíc $K \cap H = \{e\}$ a tedy $G = KH$. Pokud platí tyto vztahy, řekneme, že *G* je semidirektním součinem podgrup *K* a *H,* značíme $G = K \times_c H$. Pokud by byla *K* izomorfní s $\mathbb{Z}_4$, lze ukázat komutativitu výsledného semidirektního součinu a tedy spor. Z dalších vlastností semidirektního součinu vyplývá existence jediné

nekomutativní grupy tvaru

$$(\mathbb{Z}_2 \times \mathbb{Z}_2) \times_c H \text{, konkrétně grupy } A_4.$$

4. $s_2 = 3$, $s_3 = 1$: Podobně jako v předchozím odstavci je zde $G = K \times_c H$, kde K je řádu 3 a H je řádu 4. Dá se ukázat existence jediné grupy tvaru $\mathbb{Z}_3 \times_c \mathbb{Z}_4$, resp. $\mathbb{Z}_3 \times_c (\mathbb{Z}_2 \times \mathbb{Z}_2)$ a její izomorfnost s grupou Dic_3, resp. D_{12}.

Seznam grup malých řádů

V této části popíšeme strukturu všech nalezených grup do řádu 15 včetně. Uvedeme Cayleyho tabulky, grafy cyklů, Hasseovy diagramy znázorňující vztahy mezi podgrupami (popisy podgrup vždy následují v pořadí shora dolů a zleva doprava), dále charakterizaci grupy a případné zajímavosti.

1 Grupa řádu 1

$\mathbb{Z}_1 = S_1 = A_2$ 

$\mathbb{Z}_1 = \{e\}$

*	e
e	e

Tabulka 14: Grupa $\mathbb{Z}_1$

Obsahuje pouze jediný prvek, který je samozřejmě prvkem neutrálním. Jedná se o grupu komutativní, cyklickou, jediná podgrupa je podgrupa nevlastní. Nazývána také triviální grupou.

2 Grupa řádu 2

$\mathbb{Z}_2 = S_2 = D_2$ 

$\mathbb{Z}_2$

$\{e\}$

*	e	a
e	e	a
e	a	e

Tabulka 15: Grupa $\mathbb{Z}_2$

Nejmenší netriviální grupa, cyklická, tudíž komutativní. Izomorfní např. s podgrupou $\{I, A\}$ grupy zákrytových pohybů rovnoramenného trojúhelníku, resp. s podgrupou $\{-1, 1\}$ grupy komplexních čísel $\{-1, 1, i, -i\}$.

3 Grupa řádu 3

$\mathbb{Z}_3 = A_3$ 

$\mathbb{Z}_3$

$\{e\}$

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tabulka 16: Grupa $\mathbb{Z}_3$

Komutativní, cyklická grupa, jedinou podgrupou je podgrupa triviální. Izomorfní s podgrupou

$$\{I\,,\ L,\ R\}$$

grupy zákrytových pohybů rovnoramenného trojúhelníku, resp. s podgrupou $\{0,\ 2,\ 4\}$ grupy $\mathbb{Z}_6$.

4 Grupy řádu 4

Nejmenší řád, který jednoznačně neurčuje strukturu grupy.

$\mathbb{Z}_4$ 

$\mathbb{Z}_4$

$\mathbb{Z}_2 = \{e = a^4\,,\ a^2\}$

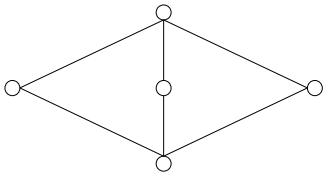
$\{e\}$

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	a	e
c	c	e	a	b

Tabulka 17: Grupa $\mathbb{Z}_4$

Cyklická, komutativní grupa. Izomorfní s grupou komplexních čísel $\{-1\,,\ 1,\ i\,,\ -i\}$.

$\mathbb{Z}_2 \times \mathbb{Z}_2 = D_4$



$\mathbb{Z}_2 \times \mathbb{Z}_2$

$\mathbb{Z}_2 = \{e,\ a\},\ \mathbb{Z}_2 = \{e,\ b\}, \mathbb{Z}_2 = \{e,\ c\}$

$\{e\}$

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Tabulka 18: Kleinova 4-grupa

Nejmenší necyklická grupa, nazývána též Kleinova čtyřgrupa. Izomorfní s grupou zákrytových pohybů obdélníku.

5 Grupa řádu 5

$\mathbb{Z}_5$

$\mathbb{Z}_5$

$\{e\}$

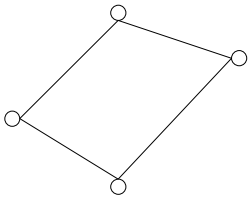
*	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Tabulka 19: Grupa $\mathbb{Z}_5$

Cyklická, komutativní grupa.

6 Grupy řádu 6

$\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$ 



$\mathbb{Z}_6$

$\mathbb{Z}_3 = \{e\,,\ a^2 = b\,,\ a^4 = d\}$

$\mathbb{Z}_2 = \{e\,,\ a^3 = c\}$

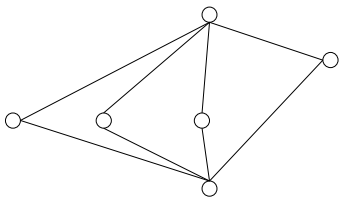
$\{e\}$

*	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

Tabulka 20: Grupa $\mathbb{Z}_6$

Cyklická, komutativní grupa.

$S_3 = D_6$ 



S_3

$\mathbb{Z}_3 = \{I,\ L,\ R\}$

$\mathbb{Z}_2 = \{I,\ A\}, \mathbb{Z}_2 = \{I,\ B\}, \mathbb{Z}_2 = \{I,\ C\}$

$\{I\}$

*	I	L	R	A	B	C
I	I	L	R	A	B	C
L	L	R	I	B	C	A
R	R	I	L	C	A	B
A	A	C	B	I	R	L
B	B	A	C	L	I	R
C	C	B	A	R	L	I

Tabulka 21: Grupa S_3

Nejmenší nekomutativní grupa. Izomorfní s grupou všech permutací 3prvkové množiny.

Poznámka: Značení prvků bylo zvoleno v souladu s příkladem, prezentovaným v této práci (grupa zákrytových pohybů rovnostranného trojúhelníku).

7 Grupa řádu 7

$\mathbb{Z}_7$ 

$\mathbb{Z}_7$

$\{e\}$

*	e	a	b	c	d	f	g
e	e	a	b	c	d	f	g
a	a	b	c	d	f	g	e
b	b	c	d	f	g	e	a
c	c	d	f	g	e	a	b
d	d	f	g	e	a	b	c
f	f	g	e	a	b	c	d
g	g	e	a	b	c	d	f

Tabulka 22: Grupa $\mathbb{Z}_7$

Cyklická, komutativní grupa.

Poznámka: Cayleyho tabulky cyklických grup již nadále uvádět nebudeme.

8 Grupy řádu 8

Existuje celkem pět grup řádu 8, tři abelovské a dvě neabelovské. Povšimněte si, že oproti nižším řádům, kdy existovaly maximálně dvě vzájemně neizomorfní grupy stejného řádu, je číslo pět vcelku značným „skokem“. Tento nárůst souvisí s tím, že číslo 8 je mocninou čísla 2, takovýto nárůst nastává i u dalších mocnin dvojky.

Například software GAP, který je určen mj. pro práci s grupami, obsahuje ve své knihovně malých grup popis všech grup do řádu 2 000 včetně, ovšem až na řád 1 024, který je také mocninou čísla 2 $(1\,024 = 2^{10})$. Jistě uhodnete, proč je právě tento řád vynechán – jenom 2-podgup řádu 1024 totiž existuje 49 487 365 422 (!) (viz [W9]).

$\mathbb{Z}_8$ 

$\mathbb{Z}_8$

$\mathbb{Z}_4 = \{e\,,\ a^2 = b,\ a^4 = d\,,\ a^6 = g\}$

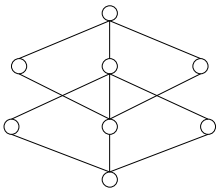
$\mathbb{Z}_2 = \{e\,,\ a^4 = d\}$

$\{e\}$

Cyklická, komutativní grupa.

$\mathbb{Z}_2 \times \mathbb{Z}_4$

Nejnázornější bude označit prvky v souladu s jejich vznikem. Prvky dílčích podgrup označíme e, f, resp. e, a, b, c, elementy direktního součinu budou uspořádanými dvojicemi těchto prvků (tyto dvojice budeme zapisovat „bez oddělovače“).



$$\mathbb{Z}_2 \times \mathbb{Z}_4$$

$$\mathbb{Z}_4 = \{ee, ea, eb, ec\},\ \mathbb{Z}_2 \times \mathbb{Z}_2 = \{ee, eb, fe, fb\},\ \mathbb{Z}_4 = \{ee, fa, eb, fc\}$$

$$\mathbb{Z}_2 = \{ee, fe\},\ \mathbb{Z}_2 = \{ee, eb\},\ \mathbb{Z}_2 = \{ee, fb\}$$

$$\{e\}$$

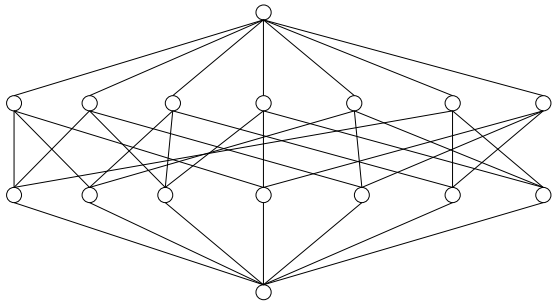
*	*ee*	*ea*	*eb*	*ec*	*fe*	*fa*	*fb*	*fc*
ee	*ee*	*ea*	*eb*	*ec*	*fe*	*fa*	*fb*	*fc*
ea	*ea*	*eb*	*ec*	*ee*	*fa*	*fb*	*fc*	*fe*
eb	*eb*	*ec*	*ee*	*ea*	*fb*	*fc*	*fe*	*fa*
ec	*ec*	*ee*	*ea*	*eb*	*fc*	*fe*	*fa*	*fb*
fe	*fe*	*fa*	*fb*	*fc*	*ee*	*ea*	*eb*	*ec*
fa	*fa*	*fb*	*fc*	*fe*	*ea*	*eb*	*ec*	*ee*
fb	*fb*	*fc*	*fe*	*fa*	*eb*	*ec*	*ee*	*ea*
fc	*fc*	*fe*	*fa*	*fb*	*ec*	*ee*	*ea*	*eb*

Tabulka 23: Grupa $\mathbb{Z}_2 \times \mathbb{Z}_4$

Komutativní grupa.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Prvky dílčích podgrup označíme e, a, resp. e, b, resp. e, c. Z těchto prvků utvoříme uspořádané trojice, opět je budeme zapisovat „bez oddělovačů“.



$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

$\{eee, aee, ebe, abe\}, \{eee, aee, eec, aec\}, \{eee, ebe, eec, ebc\}$
$\{eee, abe, eec, abc\}, \{eee, aec, ebe, abc\}, \{eee, ebc, aee, abc\}, \{eee, abe, ebc, aec\}$
$\{eee, aee\}, \{eee, ebe\}, \{eee, eec\}, \{eee, abe\}, \{eee, aec\}, \{eee, ebc\}, \{eee, abc\}$
$\{eee\}$

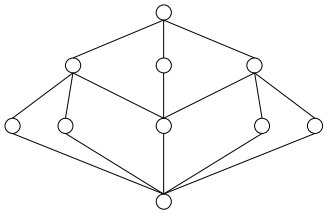
*	*eee*	*aee*	*ebe*	*abe*	*eec*	*aec*	*ebc*	*abc*
eee	*eee*	*aee*	*ebe*	*abe*	*eec*	*aec*	*ebc*	*abc*
aee	*aee*	*eee*	*abe*	*ebe*	*aec*	*eec*	*abc*	*ebc*
ebe	*ebe*	*abe*	*eee*	*aee*	*ebc*	*abc*	*eec*	*aec*
abe	*abe*	*ebe*	*aee*	*eee*	*abc*	*ebc*	*aec*	*eec*
eec	*eec*	*aec*	*ebc*	*abc*	*eee*	*aee*	*ebe*	*abe*
aec	*aec*	*eec*	*aec*	*ebc*	*aee*	*eee*	*abe*	*ebe*
ebc	*ebc*	*abc*	*eec*	*aec*	*ebe*	*abe*	*eee*	*aee*
abc	*abc*	*ebc*	*aec*	*eec*	*abe*	*ebe*	*aee*	*eee*

Tabulka 24: Grupa $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Komutativní grupa.

D_8 

Jak bylo ukázáno, prvky této grupy lze vyjádřit ve tvaru $e,\ a,\ a^2,\ a^3,\ b,\ ba,\ ba^2,\ ba^3$.



D_8

$\{e,\ a^2,\ ba^2,\ b\},\ \mathbb{Z}_4 = \{e,\ a,\ a^2,\ a^3\},\ \{e,\ a^2,\ ba,\ ba^3\}$

$\{e,\ ba^2\},\ \{e,\ b\},\ \{e,\ a^2\},\ \{e,\ ba\}\ \{e,\ ba^3\}$

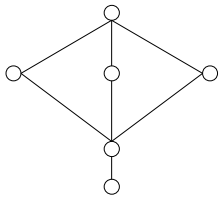
$\{e\}$

*	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	e	a	a^2	a^3
ba	ba	ba^2	ba^3	b	a^3	e	a	a^2
ba^2	ba^2	ba^3	b	ba	a^2	a^3	e	a
ba^3	ba^3	b	ba	ba^2	a	a^2	a^3	e

Tabulka 25: Grupa D_8

Nekomutativní grupa. Izomorfní s grupou zákrytových pohybů čtverce, na mocniny prvku a lze nahlížet jako na rotace, zbylé prvky reprezentují osové souměrnosti.

Q 



Q

$\{1, -1, i, -i\}, \{1, -1, j, -j\}, \{1, -1, k, -k\}$

$\{1, -1\}$

$\{1\}$

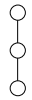
*	1	–1	i	$-i$	j	$-j$	k	$-k$
1	1	–1	i	$-i$	j	$-j$	k	$-k$
–1	–1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	–1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	–1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	–1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	–1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	–1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	–1

Tabulka 26: Grupa Q

Nekomutativní grupa. Nazývána grupa kvaternionů. Nejmenší nekomutativní grupa, mající pouze normální podgrupy – tzv. *Hamiltonovská grupa* (jistým protipólem Hamiltonovské podgrupy je jednoduchá grupa, viz kapitola s příklady grup).

9 Grupy řádu 9

$\mathbb{Z}_9$ 



$\mathbb{Z}_9$

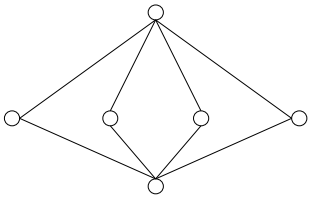
$\mathbb{Z}_3 = \{e, a^3, a^6\}$

$\{e\}$

Cyklická, tedy komutativní grupa.

$\mathbb{Z}_3 \times \mathbb{Z}_3$ 

Prvky dvou dílčích podgrup označíme e, a, a^2, resp. e, a, a^2. Prvky výsledné grupy lze vyjádřit jako uspořádané dvojice prvků dílčích grup.



$$\mathbb{Z}_3 \times \mathbb{Z}_3$$
$$\{ee,\ ae,\ a^2e\},\ \{ee,\ eb,\ eb^2\},\{ee,\ ab,\ a^2b^2\},\ \{ee,\ ab^2,\ a^2b\}$$
$$\{ee\}$$

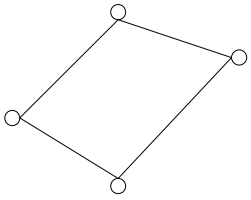
*	ee	eb	eb^2	ae	ab	ab^2	a^2e	a^2b	a^2b^2
ee	ee	eb	eb^2	ae	ab	ab^2	a^2e	a^2b	a^2b^2
eb	eb	eb^2	ee	ab	ab^2	ae	a^2b	a^2b^2	a^2e
eb^2	eb^2	ee	eb	ab^2	ae	ab	a^2b^2	a^2e	a^2b
ae	ae	ab	ab^2	a^2e	a^2b	a^2b^2	ee	eb	eb^2
ab	ab	ab^2	ae	a^2b	a^2b^2	a^2e	eb	eb^2	ee
ab^2	ab^2	ae	ab	a^2b^2	a^2e	a^2b	eb^2	ee	eb
a^2e	a^2e	a^2b	a^2b^2	ee	eb	eb^2	ae	ab	ab^2
a^2b	a^2b	a^2b^2	a^2e	eb	eb^2	ee	ab	ab^2	ae
a^2b^2	a^2b^2	a^2e	a^2b	eb^2	ee	eb	ab^2	ae	ab

Tabulka 27: Grupa $\mathbb{Z}_3 \times \mathbb{Z}_3$

Necyklická komutativní grupa.

10 Grupy řádu 10

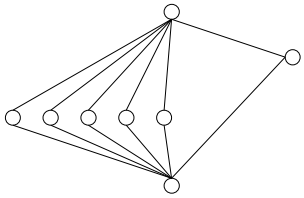
$\mathbb{Z}_{10} = \mathbb{Z}_2 \times \mathbb{Z}_5$ 



$$\mathbb{Z}_{10}$$
$$\mathbb{Z}_5 = \{e,\ a^2,\ a^4,\ a^6,\ a^8\}$$
$$\mathbb{Z}_2 = \{e,\ a^5\}$$
$$\{e\}$$

Cyklická grupa.

D_{10} 



Prvky této grupy lze vyjádřit ve tvaru e, a, a^2, a^3, a^4, b, ba, ba^2, ba^3, ba^4.

$$D_{10}$$
$$\mathbb{Z}_5 = \{e, a, a^2, a^3, a^4\}$$
$$\{e, b\}, \{e, ba\}, \{e, ba^2\}, \{e, ba^3\}\ \{e, ba^4\}$$
$$\{e\}$$

*	e	a	a^2	a^3	a^4	b	ba	ba^2	ba^3	ba^4
e	e	a	a^2	a^3	a^4	b	ba	ba^2	ba^3	ba^4
a	a	a^2	a^3	a^4	e	ba^4	b	ba	ba^2	ba^3
a^2	a^2	a^3	a^4	e	a	ba^3	ba^4	b	ba	ba^2
a^3	a^3	a^4	e	a	a^2	ba^2	ba^3	ba^4	b	ba
a^4	a^4	e	a	a^2	a^3	ba	ba^2	ba^3	ba^4	ba^3
b	b	ba	ba^2	ba^3	ba^4	e	a	a^2	a^3	a^4
ba	ba	ba^2	ba^3	ba^4	b	a^4	e	a	a^2	a^3
ba^2	ba^2	ba^3	ba^4	b	ba	a^3	a^4	e	a	a^2
ba^3	ba^3	ba^4	b	ba	ba^2	a^2	a^3	a^4	e	a
ba^4	ba^4	b	ba	ba^2	ba^3	a	a^2	a^3	a^4	e

Tabulka 28: Grupa D_{10}

Nekomutativní grupa. Izomorfní s grupou zákrytových pohybů pravidelného pětiúhelníku, na mocniny prvku a lze nahlížet jako na rotace, zbylé prvky reprezentují osové souměrnosti.

11 Grupa řádu 11

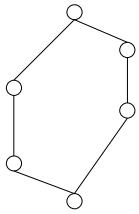
$\mathbb{Z}_{11}$ 

$$\mathbb{Z}_{11}$$
$$\{e\}$$

Cyklická, komutativní grupa.

12 Grupy řádu 12

$\mathbb{Z}_{12} = \mathbb{Z}_3 \times \mathbb{Z}_4$ 

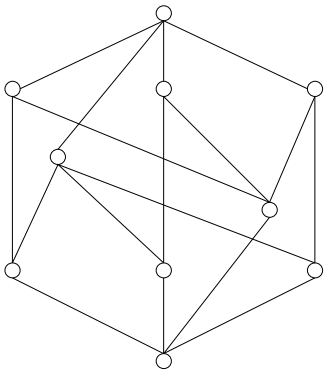


$\mathbb{Z}_{12}$
$\mathbb{Z}_6$
$\mathbb{Z}_4$
$\mathbb{Z}_3$
$\mathbb{Z}_2$
$\{e\}$

Cyklická, komutativní grupa.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ 

Prvky dílčích podgrup označíme e, f, resp. e, g, resp. e, a, a^2. Z těchto prvků utvoříme uspořádané trojice, opět je budeme zapisovat „bez oddělovačů“.



$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$

$\{eee, eea, eea^2, ege, ega, ega^2\}, \{eee, eea, eea^2, fee, fea, fea^2\}$

$\{eee, fga, eea^2, fge, eea, fga^2\}$

$\{eee, fee, ege, fge\}$

$\{eee, eea, eea^2\}$

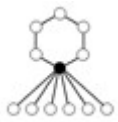
$\{eee, ege\}, \{eee, fee\}, \{eee, fge\}$

$\{e\}$

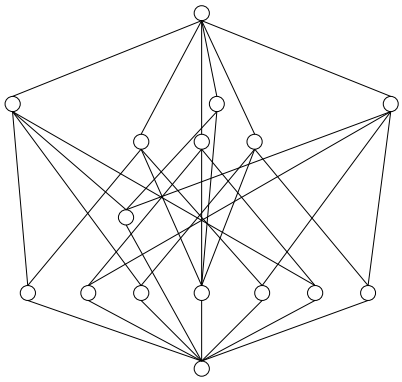
*	eee	eea	eea^2	ege	ega	ega^2	fee	fea	fea^2	fge	fga	fga^2
eee	eee	eea	eea^2	ege	ega	ega^2	fee	fea	fea^2	fge	fga	fga^2
eea	eea	eea^2	eee	ega	ega^2	ege	fea	fea^2	fee	fga	fga^2	fge
eea^2	eea^2	eee	eea	ega^2	ege	ega	fea^2	fee	fea	fga^2	fge	fga
ege	ege	ega	ega^2	eee	eea	eea^2	fge	fga	fga^2	fee	fea	fea^2
ega	ega	ega^2	ege	eea	eea^2	eee	fga	fga^2	fge	fea	fea^2	fee
ega^2	ega^2	eea^2	ega	eea^2	eee	eea	fga^2	fge	fga	fea^2	fee	fea
fee	fee	fea	fea^2	fge	fga	fga^2	eee	eea	eea^2	ege	ega	ega^2
fea	fea	fea^2	fee	fga	fga^2	fge	eea	eea^2	eee	ega	ega^2	ege
fea^2	fea^2	fee	fea	fga^2	fge	fga	eea^2	eee	eea	ega^2	ege	ega
fge	fge	fga	fga^2	fee	fea	fea^2	ege	ega	ega^2	eee	eea	eea^2
fga	fga	fga^2	fge	fea	fea^2	fee	ega	ega^2	ege	eea	eea^2	eee
fga^2	fga^2	fge	fga	fea^2	fee	fea	ega^2	ege	ega	eea^2	eee	eea

Tabulka 29: Grupa $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$

Komutativní grupa.

D_{12} 

Prvky této grupy lze vyjádřit ve tvaru $e,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ b,\ ba,\ ba^2,\ ba^3,\ ba^4,\ ba^5$.



D_{12}

$D_6 = \{e,\ a^2,\ a^4,\ b,\ ba^2,\ ba^4\},\ \mathbb{Z}_6 = \{e,\ a,\ a^2,\ a^3,\ a^4,\ a^5\},\ D_6 = \{e,\ a^2,\ a^4,\ ba,\ ba^3,\ ba^5\}$

$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{e,\ a^3,\ b,\ ba^3\},\ \mathbb{Z}_2 \times \mathbb{Z}_2 = \{e,\ a^3,\ ba,\ ba^4\},\ \mathbb{Z}_2 \times \mathbb{Z}_2 = \{e,\ a^3,\ ba^2,\ ba^5\}$

$\mathbb{Z}_3 = \{e,\ a^2,\ a^4\}$

$\{e,\ b\},\ \{e,\ ba\},\ \{e,\ ba^2\},\ \{e,\ a^3\},\ \{e,\ ba^3\},\ \{e,\ ba^4\},\ \{e,\ ba^5\}$

$\{e\}$

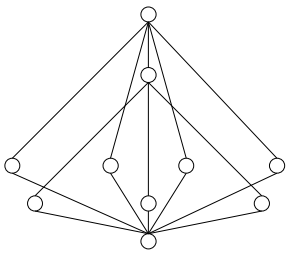
*	e	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5
e	e	a	a^2	a^3	a^4	a^5	b	ba	ba^2	ba^3	ba^4	ba^5
a	a	a^2	a^3	a^4	a^5	e	ba^5	b	ba	ba^2	ba^3	ba^4
a^2	a^2	a^3	a^4	a^5	e	a	ba^4	ba^5	b	ba	ba^2	ba^3
a^3	a^3	a^4	a^5	e	a	a^2	ba^3	ba^4	ba^5	b	ba	ba^2
a^4	a^4	a^5	e	a	a^2	a^3	ba^2	ba^3	ba^4	ba^5	b	ba
a^5	a^5	e	a	a^2	a^3	a^4	ba	ba^2	ba^3	ba^4	ba^5	b
b	b	ba	ba^2	ba^3	ba^4	ba^5	e	a	a^2	a^3	a^4	a^5
ba	ba	ba^2	ba^3	ba^4	ba^5	b	a^5	e	a	a^2	a^3	a^4
ba^2	ba^2	ba^3	ba^4	ba^5	b	ba	a^4	a^5	e	a	a^2	a^3
ba^3	ba^3	ba^4	ba^5	b	ba	ba^2	a^3	a^4	a^5	e	a	a^2
ba^4	ba^4	ba^5	b	ba	ba^2	ba^3	a^2	a^3	a^4	a^5	e	a
ba^5	ba^5	b	ba	ba^2	ba^3	ba^4	a	a^2	a^3	a^4	a^5	e

Tabulka 30: Grupa D_{12}

Nekomutativní grupa. Izomorfní s grupou zákrytových pohybů pravidelného šestiúhelníku, na mocniny prvku a lze nahlížet jako na rotace, zbylé prvky reprezentují osové souměrnosti.

A_4 

Grupu lze vyjádřit jako podgrupu všech sudých permutací symetrické grupy S_4. Permutujme prvky $1, 2, 3, 4$.



A_4

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(1), (12)(34), (13)(24), (14)(23)\}$$
$$\{(1), (123), (132)\}, \{(1), (124), (142)\}, \{(1), (134), (143)\}, \{(1), (234), (243)\}$$
$$\{(1), (12)(34)\}, \{(1), (13)(24)\}, \{(1), (14)(23)\}$$
$$\{e\}$$

*	(1)	(123)	(132)	(124)	(142)	(134)	(143)	(234)	(243)	(12)(34)	(13)(24)	(14)(23)
(1)	(1)	(123)	(132)	(124)	(142)	(134)	(143)	(234)	(243)	(12)(34)	(13)(24)	(14)(23)
(123)	(123)	(132)	(1)	(14)(23)	(234)	(124)	(12)(34)	(13)(24)	(143)	(243)	(142)	(134)
(132)	(132)	(1)	(123)	(134)	(13)(24)	(14)(23)	(243)	(142)	(12)(34)	(143)	(234)	(124)
(124)	(124)	(13)(24)	(243)	(142)	(1)	(12)(34)	(123)	(134)	(14)(23)	(234)	(143)	(132)
(142)	(142)	(143)	(14)(23)	(1)	(124)	(234)	(13)(24)	(12)(34)	(132)	(134)	(123)	(243)
(134)	(134)	(234)	(12)(34)	(13)(24)	(132)	(143)	(1)	(14)(23)	(124)	(142)	(243)	(123)
(143)	(143)	(14)(23)	(142)	(243)	(12)(34)	(1)	(134)	(123)	(13)(24)	(132)	(124)	(234)
(234)	(234)	(12)(34)	(134)	(123)	(14)(23)	(13)(24)	(142)	(243)	(1)	(124)	(132)	(143)
(243)	(243)	(124)	(13)(24)	(12)(34)	(143)	(132)	(14)(23)	(1)	(234)	(123)	(134)	(142)
(12)(34)	(12)(34)	(134)	(234)	(143)	(243)	(123)	(124)	(132)	(142)	(1)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(243)	(124)	(132)	(134)	(142)	(234)	(143)	(123)	(14)(23)	(1)	(12)(34)
(14)(23)	(14)(23)	(142)	(142)	(234)	(123)	(243)	(132)	(124)	(134)	(13)(24)	(12)(34)	(1)

Tabulka 31: Grupa A_4

Poznámka: Tabulka částečně převzata z [W10].

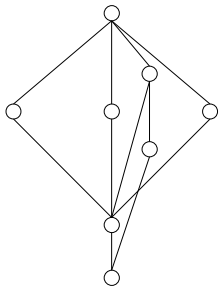
Nekomutativní grupa. Nazývána alternující grupa. Nejmenší grupa, která nemá podgrupy všech řádů dělících řád grupy (neexistuje podgrupa řádu 6). Tím je vyvrácena platnost opačné implikace k Lagrangeově větě. Povšimněte si, že (v souladu s 1. Sylowovou větou) grupa má podgrupy řádů 2, 3, resp. 4, neboť tyto řády jsou prvočísly, resp. mocninou prvočísla dělícího řád grupy.

Dic_3 

Jak bylo ukázáno, prvky této grupy lze vyjádřit ve tvaru

$$\{e,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ b,\ ab,\ a^2b,\ a^3b,\ a^4b,\ a^5b\}$$

spolu s násobením $b^2 = a^3,\ ba = a^{-1}b$.



Dic_3

$$\mathbb{Z}_6 = \{e,\ a,\ a^2,\ a^3,\ a^4,\ a^5\}$$

$$\mathbb{Z}_4 = \{e,\ b,\ a^3,\ a^3b\},\ \mathbb{Z}_4 = \{e,\ ab,\ a^3,\ a^4b\},\ \mathbb{Z}_4 = \{e,\ a^2b,\ a^3,\ a^5b\}$$

$$\mathbb{Z}_3 = \{e,\ a^2,\ a^4\}$$

$$\mathbb{Z}_2 = \{e,\ a^3\}$$

$$\{e\}$$

*	e	a	a^2	a^3	a^4	a^5	b	ab	a^2b	a^3b	a^4b	a^5b
e	e	a	a^2	a^3	a^4	a^5	b	ab	a^2b	a^3b	a^4b	a^5b
a	a	a^2	a^3	a^4	a^5	e	ab	a^2b	a^3b	a^4b	a^5b	b
a^2	a^2	a^3	a^4	a^5	e	a	a^2b	a^3b	a^4b	a^5b	b	ab
a^3	a^3	a^4	a^5	e	a	a^2	a^3b	a^4b	a^5b	b	ab	a^2b
a^4	a^4	a^5	e	a	a^2	a^3	a^4b	a^5b	b	ab	a^2b	a^3b
a^5	a^5	e	a	a^2	a^3	a^4	a^5b	b	ab	a^2b	a^3b	a^4b
b	b	a^5b	a^4b	a^3b	a^2b	ab	a^3	a^2	a	e	a^5	a^4
ab	ab	b	a^5b	a^4b	a^3b	a^2b	a^4	a^3	a^2	a	e	a^5
a^2b	a^2b	ab	b	a^5b	a^4b	a^3b	a^5	a^4	a^3	a^2	a	e
a^3b	a^3b	a^2b	ab	b	a^5b	a^4b	e	a^5	a^4	a^3	a^2	a
a^4b	a^4b	a^3b	a^2b	ab	b	a^5b	a	e	a^5	a^4	a^3	a^2
a^5b	a^5b	a^4b	a^3b	a^2b	ab	b	a^2	a	e	a^5	a^4	a^3

Tabulka 32: Grupa Dic_3

Nekomutativní grupa.

13 Grupa řádu 13

$\mathbb{Z}_{13}$ 

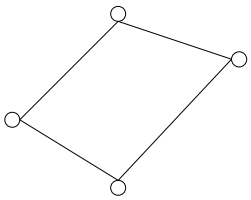
$\mathbb{Z}_{13}$

$\{e\}$

Cyklická, komutativní grupa.

14 Grupy řádu 14

$\mathbb{Z}_{14} = \mathbb{Z}_2 \times \mathbb{Z}_7$ 



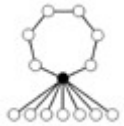
$\mathbb{Z}_{14}$

$\mathbb{Z}_7 = \{e,\ a^2,\ a^4,\ a^6,\ a^8,\ a^{10},\ a^{12}\}$

$\mathbb{Z}_2 = \{e,\ a^7\}$

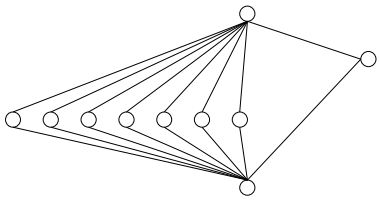
$\{e\}$

Cyklická, komutativní grupa.

D_{14} 

Prvky této grupy lze vyjádřit ve tvaru

$$e,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6,\ b,\ ba,\ ba^2,\ ba^3,\ ba^4,\ ba^5,\ ba^6\ .$$



$$D_{14}$$
$$\mathbb{Z}_7 = \{e,\ a,\ a^2,\ a^3,\ a^4,\ a^5,\ a^6\}$$
$$\{e,\ b\},\ \{e,\ ba\},\ \{e,\ ba^2\},\ \{e,\ ba^3\}\ \{e,\ ba^4\},\ \{e,\ ba^5\},\ \{e,\ ba^6\}$$
$$\{e\}$$

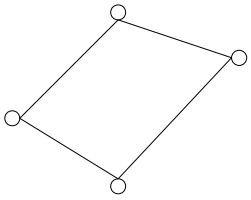
*	e	a	a^2	a^3	a^4	a^5	a^6	b	ba	ba^2	ba^3	ba^4	ba^5	ba^6
e	e	a	a^2	a^3	a^4	a^5	a^6	b	ba	ba^2	ba^3	ba^4	ba^5	ba^6
a	a	a^2	a^3	a^4	a^5	a^6	e	ba^6	b	ba	ba^2	ba^3	ba^4	ba^5
a^2	a^2	a^3	a^4	a^5	a^6	e	a	ba^5	ba^6	b	ba	ba^2	ba^3	ba^4
a^3	a^3	a^4	a^5	a^6	e	a	a^2	ba^4	ba^5	ba^6	b	ba	ba^2	ba^3
a^4	a^4	a^5	a^6	e	a	a^2	a^3	ba^3	ba^4	ba^5	ba^6	b	ba	ba^2
a^5	a^5	a^6	e	a	a^2	a^3	a^4	ba^2	ba^3	ba^4	ba^5	ba^6	b	ba
a^6	a^6	e	a	a^2	a^3	a^4	a^5	ba	ba^2	ba^3	ba^4	ba^5	ba^6	b
b	b	ba	ba^2	ba^3	ba^4	ba^5	ba^6	e	a	a^2	a^3	a^4	a^5	a^6
ba	ba	ba^2	ba^3	ba^4	ba^5	ba^6	b	a^6	e	a	a^2	a^3	a^4	a^5
ba^2	ba^2	ba^3	ba^4	ba^5	ba^6	b	ba	a^5	a^6	e	a	a^2	a^3	a^4
ba^3	ba^3	ba^4	ba^5	ba^6	b	ba	ba^2	a^4	a^5	a^6	e	a	a^2	a^3
ba^4	ba^4	ba^5	ba^6	b	ba	ba^2	ba^3	a^3	a^4	a^5	a^6	e	a	a^2
ba^5	ba^5	ba^6	b	ba	ba^2	ba^3	ba^4	a^2	a^3	a^4	a^5	a^6	e	a
ba^6	ba^6	b	ba	ba^2	ba^3	ba^4	ba^5	a	a^2	a^3	a^4	a^5	a^6	e

Tabulka 33: Grupa D_{14}

Nekomutativní grupa. Izomorfní s grupou zákrytových pohybů pravidelného sedmiúhelníku, na mocniny prvku a lze nahlížet jako na rotace, zbylé prvky reprezentují osové souměrnosti.

15 Grupa řádu 15

$\mathbb{Z}_{15} = \mathbb{Z}_3 \times \mathbb{Z}_5$ 



$\mathbb{Z}_{15}$

$\mathbb{Z}_5 = \{e,\ a^3,\ a^6,\ a^9,\ a^{12}\}$

$\mathbb{Z}_3 = \{e,\ a^5,\ a^{10}\}$

$\{e\}$

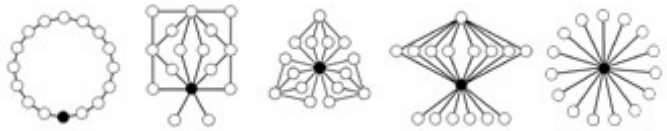
Cyklická, komutativní grupa.

Grupy vyšších řádů

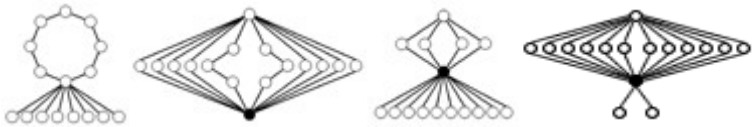
Práce věnující se popisu grup malých řádů obvykle končí u čísla 15. Z předchozího textu by měl být patrný důvod – řád 16 je roven mocnině čísla 2, proto existuje poměrně velký počet vzájemně neizomorfních grup tohoto řádu. Konkrétně se jedná o 5 grup komutativních a 9 grup nekomutativních. Následuje jejich stručný přehled (obrázky převzaty z [W9]).

Nejprve se zaměřme na abelovské grupy. Jedná se o direktní součiny

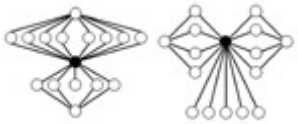
$$\mathbb{Z}_{16},\ \mathbb{Z}_8 \times \mathbb{Z}_2,\ \mathbb{Z}_4 \times \mathbb{Z}_4,\ \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 .$$



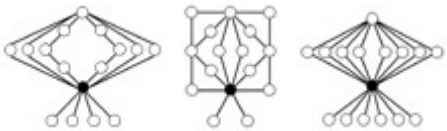
Co se týče nám „známých“ nekomutativních grup, na prvním místě je dihedrální grupa D_{16}, následují dicyklická grupa Dic_4 a direktní součiny $Dih_4 \times \mathbb{Z}_2$ a $Q \times \mathbb{Z}_2$.



O semidirektním součinu grup jsme se zmiňovali již v části o grupách řádu 12, tímto způsobem jsou utvořeny grupy $\mathbb{Z}_4 \times_c \mathbb{Z}_4$ a $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times_c \mathbb{Z}_4$.



Zbývají tři grupy – kvazidihedrální grupa, modulární grupa a grupa generovaná tzv. *Pauliho maticemi*.



Povšimněte si, že poslední dvě grupy mají stejný graf cyklů jako grupy

$$\mathbb{Z}_8 \times \mathbb{Z}_2 \text{, resp. } \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 .$$

Z toho vyplývá, že zde graf cyklů jednoznačně neurčuje grupu.

Stručně se pozastavíme nad řády 17 až 20. Řády 17 a 19 jsou prvočísla, odpovídají jim tedy pouze grupy $\mathbb{Z}_{17}$, resp. $\mathbb{Z}_{19}$.

Existuje 5 vzájemně neizomorfních grup řádu 18, z toho 2 abelovské,

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \text{ a } \mathbb{Z}_2 \times \mathbb{Z}_9 .$$

Ze tří neabelovských grup zmiňme dihedrální grupu D_{18}.

U řádu 20 je situace analogická – nalezneme zde komutativní grupy

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \text{ a } \mathbb{Z}_4 \times \mathbb{Z}_5 ,$$

též tři nekomutativní grupy, z nichž je pro nás nejznámější grupa D_{20}.

Údaje o počtech grup daných řádů přináší následující tabulka (*K*, resp. *N* znamená počet komutativních, resp. nekomutativních grup):

řád	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Σ
K	1	1	1	2	1	1	1	3	2	1	1	2	1	1	1	5	1	2	1	2	31
N	0	0	0	0	0	1	0	2	0	1	0	3	0	1	0	9	0	3	0	3	23
Σ	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1	5	54

Tabulka 34: Počty grup jednotlivých řádů

Příklady grup

V této kapitole ukážeme některé z oblastí, v nichž se můžeme setkat s grupami. Každé z následujících témat by jistě vydalo na samostatnou práci, zde se omezíme pouze na hrubé naznačení problematiky.

1 Geometrické transformace

V tomto odvětví geometrie lze nalézt celou řadu grup. Připomeňme nejprve pojem afinita. Nechť je dán afinní prostor A_n dimenze n spolu se soustavou souřadnic. Afinitou tohoto prostoru rozumíme bijekci $f: A_n \to A_n$

$$f\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Velmi zhruba řečeno, afinita „zachovává kolinearitu a dělicí poměr“. Lze ukázat, že všechny afinity daného afinního prostoru tvoří grupu – jedním z klíčových postřehů při důkazu je fakt, že požadavek na vzájemnou jednoznačnost zobrazení odpovídá požadavku na regulárnost výše uvedené matice.

Přejdeme-li od afinního prostoru k prostoru eukleidovskému, lze hovořit o vzdálenosti bodů. Afinitě daného eukleidovského prostoru, která zachovává vzdálenosti bodů, říkáme shodnost. Zobrazení $f: E_n \to E_n$ je shodností právě tehdy, když jemu příslušná matice A je ortogonální, tj.

$$A A^T = I.$$

Opět se ukazuje, že všechny shodnosti daného prostoru tvoří grupu. Protože determinant matice je roven determinantu matice transponované, musí platit $det(A) = \pm 1$. Pokud $det(A) = 1$, resp. $det(A) = -1$, hovoříme o přímé, resp. nepřímé shodnosti. Přímé shodnosti tvoří podgrupu grupy všech shodností, nepřímé nikoliv (neboť determinant neutrálního prvku, tj. jednotkové matice, je roven jedné).

Zachování vzdáleností lze vyjádřit ve tvaru

$$|f(X) f(Y)| = |XY|.$$

Spokojíme-li se se slabší podmínkou

$$|f(X) f(Y)| = k \cdot |XY|;\ k > 0,$$

hovoříme o podobnosti. Rovnost $A A^T = I$ je v tomto případě nahrazena rovností $A A^T = k^2 \cdot I$. I množina všech podobností daného eukleidovského prostoru spolu s operací skládání zobrazení tvoří grupu.

Z dalších grup transformací uveďme například grupu posunutí (translací), grupu stejnolehlostí s daným středem. Množina všech stejnolehlostí grupu netvoří, ovšem množina všech stejnolehlostí a posunutí již ano, nazýváme ji grupa homotetií.

Předchozí myšlenky uvedl již F. Klein v roce 1872 ve své slavné přednášce, tzv. *Erlangenském programu*, rozvedl ji však ještě mnohem dále.

Cílem jeho přednášky bylo zejména vymezení a logické uspořádání jednotlivých geometrií.

Při zkoumání geometrií přirozeně vyvstává otázka, jak jednotlivé geometrie definovat, jak vysvětlit, čím se zabývají. Lze například říci, že eukleidovská geometrie se zabývá pouze těmi vlastnostmi útvarů, které se nemění při „pohybech“ těchto útvarů, v tomto případě při libovolné shodnosti. Grupa těchto pohybů dává vzniknout ekvivalenci geometrických útvarů – např. dva trojúhelníky považujeme v eukleidovské geometrii za ekvivalentní (shodné), existuje-li pohyb (shodnost), kterým lze přenést jeden trojúhelník na druhý.

Geometrii lze na základě předchozích úvah definovat jako teorii invariantů jisté grupy transformací. Touto definicí je přirozeně vyřešen i druhý úkol Erlangenského programu – geometrie lze uspořádat podle vzájemné inkluze příslušných grup transformací.

Víme-li tedy, že grupa shodností daného prostoru je podgrupou grupy podobností, lze říci, že „podobnostní“ geometrie je podmnožinou geometrie shodností. Na první pohled nelogické obrácení inkluze vyplývá z definice geometrie. Jedná se teorii invariantů jisté grupy, zvolíme-li tudíž nadgrupu této grupy, množina invariantů se logicky zmenší (viz [11], str. 67–81).

2 Grupa uzavřených cest

Pro popis této grupy využijeme příkladu uvedeného mj. v [7], str. 107–109, který se věnuje otázkám průchodu bludištěm. Představme si bludiště a Herakla stojícího v libovolném místě tohoto bludiště. Uvažujme nyní jeho všechny možné „procházky“ po bludišti vracející se na původní místo, nadále jim říkejme cesty. V průběhu cesty může hrdina projít každým místem (včetně místa výchozího) vícekrát, může se též vracet po vlastních stopách. Jak je jeho zvykem, po cestě bude odvinovat nit (i po cestě zpět po vlastních stopách), aby označil, kolikrát prošel danými částmi bludiště.

Pokusme se nyní vytvořit grupu, jejímiž prvky budou právě všechny cesty po daném bludišti vracející se do daného bodu. Jako grupová operace se nabízí „zřetězení“ cest. Zřetězením dvou cest vznikne opět cesta, neutrálním prvkem je cesta, při které vůbec neopustíme výchozí místo. Při hledání inverzních prvků ovšem nastává problém – k žádné cestě, která opustí výchozí místo, neexistuje cesta inverzní. Důvod je zřejmý – hrdina nit neustále odvinuje, pokud tedy opustí výchozí místo, nemůže již nastat situace, že žádná nit nebude odvinutá.

Jako přirozenější se jeví opětovně nit namotávat, vrací-li se hrdina zpět po svých stopách. V tomto případě z cesty vyloučíme úseky, které sice hrdina prošel, ale vzápětí se po nich vrátil zpět, tedy úseky, které po ukončení cesty nejsou označeny nití. Při tomto zobecnění již lze ke každé cestě najít cestu inverzní – stačí „projít původní cestu v protisměru“. Takto definované cesty spolu s operací zřetězení cest tedy tvoří grupu.

3 Galoisova grupa

Uvažujme kvadratickou rovnici

$$x^2 + ax + b = 0 \text{ a její kořeny } x_1,\ x_2\,.$$

Z rozkladu na součin

$$x^2 + ax + b = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2) + x_1 x_2 \text{ je zřejmé,}$$

že pro koeficienty a, b platí rovnosti

$$a = -(x_1 + x_2),\ b = x_1 x_2\,.$$

Pro nalezení kořenů používáme vzorce

$$x_1,\ x_2 = \frac{-a \pm \sqrt{a^2 - 4\mathrm{b}}}{2}\ .$$

Při postupném dosazování za koeficienty *a*, *b* do předchozího výrazu získáváme rovnosti

$$\begin{aligned} a^2 &= (x_1 + x_2)^2, \\ a^2 - 4\mathrm{b} &= x_1^2 - 2\mathrm{x}_1 x_2 + x_2^2, \\ \sqrt{a^2 - 4\mathrm{b}} &= \pm(x_1 - x_2), \\ \frac{-a \pm \sqrt{a^2 - 4\mathrm{b}}}{2} &= x_1, \text{ resp. } x_2. \end{aligned}$$

Poznamenejme, že dva (různé) kořeny získáváme na základě „odmocnění“ rovnice. Důležitější je pro nás však jiný fakt – první dva výrazy nemění hodnotu při permutaci kořenů, tato symetrie je narušena až odmocněním. Pokud se nad problémem zamyslíme, dospějeme k závěru, že symetrická bude jistě libovolná algebraická funkce utvořená z koeficientů. Úkolem řešitele kvadratické rovnice je tuto symetrii odstranit – hledáme totiž nesymetrické výrazy $x_1,\ x_2$.

Zatím jsme uvažovali pouze algebraické výrazy utvořené z koeficientů kvadratické rovnice (výrazy $a^2,\ a^2 - 4\mathrm{b}$). (Samozřejmě se nemusíme omezovat pouze na kvadratické rovnice, lze hledat kořeny polynomu libovolného stupně.) Utvořené výrazy, jak již bylo řečeno, nemění hodnotu při *libovolné* permutaci kořenů.

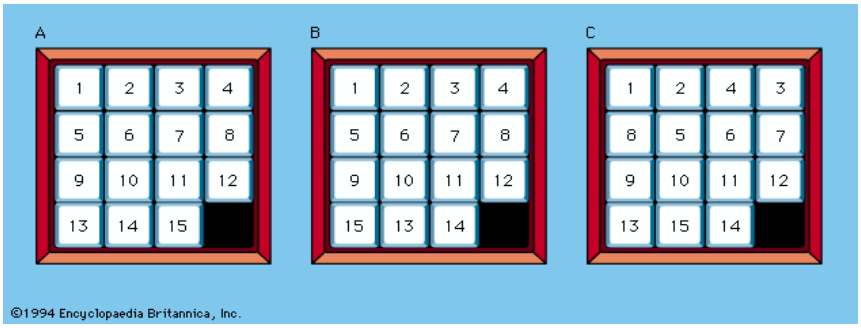
Uvažujme nyní polynom stupně *n* nad daným tělesem *T* a jeho kořeny $x_1,\ x_2,\ \ldots,\ x_n$. Nechť je dána algebraická rovnice *n* proměnných s koeficienty z tělesa *T* a nechť *n*-tice $x_1,\ x_2,\ \ldots,\ x_n$ je řešením této rovnice. Zřejmě obecně neplatí, že i libovolná permutace prvků $x_1,\ x_2,\ \ldots,\ x_n$ řeší danou rovnici. Vezměme tedy pouze ty permutace kořenů daného polynomu, které tuto podmínku splňují pro *každou* algebraickou rovnici *n* proměnných s koeficienty z tělesa *T*. Lze ukázat, že množina všech těchto permutací spolu s operací skládání permutací tvoří grupu. Tuto grupu nazýváme Galoisovou grupou daného polynomu.

Na základě zkoumání Galoisových grup lze mj. ukázat, že neexistuje obdoba vzorce pro výpočet kořenů kvadratické rovnice pro rovnice pátého či vyššího stupně (viz [W10]).

4 Hlavolamy

Velice zajímavou aplikací teorie grup v praxi jsou různé hříčky a hlavolamy, např. patnáctka, spočívající v řazení patnácti číslovaných kamenů uvnitř čtvercové hrací plochy.

Při úvahách o této hříčce využijeme grupu permutací 16 prvků (prázdné pole si můžeme představit jako prvek s číslem 16). Lze ukázat, že ze základní pozice můžeme složit právě liché permutace s prázdným polem na lichém místě, resp. sudé permutace s prázdným polem na sudém místě. Druhá pozice na následujícím obrázku je tedy řešitelná, třetí nikoliv. Zmíněná neřešitelná pozice stojí za někdejší popularitou této hříčky – na vyřešení této pozice byla vypsána odměna ve výši $ 1000.



Obrázek 2: Hra „patnáct“

Dále se zaměříme na tzv. *Rubikovu kostku*, a to v její základní podobě. Jedná se o krychli, složenou z 27 menších krychliček. Úkolem řešitele je přeskládat tyto krychličky takovým způsobem, aby všechny stěny Rubikovy kostky byly jednobarevné.

Tahem budeme rozumět jakoukoliv (i prázdnou) posloupnost operací na Rubikově kostce, tedy např. „pootoč horní vrstvu o 90° po směru hodinových ručiček, poté spodní vrstvu o 180°“. Složením dvou tahů P, Q rozumíme jejich provedení v tomto pořadí. Lze ukázat, že tahy na Rubikově kostce spolu se skládáním tvoří grupu – neutrálním prvkem je „nulový tah“, složením tahů vzniká opět tah, konečně každý tah můžeme „anulovat“ provedením inverzních operací v opačném pořadí.

Obrázek 3: Rubikova kostka

Je třeba rozlišovat mezi tahem a pozicí – tah jsme právě definovali, pozicí rozumíme vzájemnou polohu dílčích krychliček. Základní pozicí potom rozumíme libovolnou pevně zvolenou pozici, ve které je kostka považována za „vyřešenou“ tj. všechny stěny krychle jsou jednobarevné. Řešitelnou pozicí nazveme pozici, ze které můžeme posloupností tahů přejít do základní pozice. Snadno se uváží, že řešitelné jsou právě pozice, které lze vytvořit posloupností tahů z pozice základní.

Při dalším zkoumání Rubikovy kostky lze jejích 26 krychlí (neuvažujeme dále krychli skrytou uvnitř kostky) rozdělit do tří tříd. První třídu tvoří rohové kostičky (8), druhou kostičky hranové (12), třetí kostičky stěnové (6). Zřejmě příslušnost do dané třídy nezáleží na konkrétní pozici Rubikovy krychle, jinak řečeno, při skládání pouze „permutujeme“ kostičky v rámci jejich tříd.

Třetí zmíněná třída se od předchozích liší – stěnové kostičky se při skládání kostky pouze otáčejí, jejich vzájemná poloha se nemění, na jejich základě lze tedy vybudovat „souřadný systém“.

Odhlédneme-li od přesné orientace kostiček, tedy budeme-li se zajímat pouze o jejich vzájemnou polohu, lze jednotlivé operace i tahy vyjádřit pomocí permutací. Ukazuje se, že každá základní operace vytváří dva cykly délky 4 a ostatní cykly délky 1, tedy sudou permutaci. Jelikož skládáním sudých permutací vzniká opět sudá permutace, dospíváme k závěru, že všechny liché permutace na Rubikově kostce jsou neřešitelné.

Klíčovou permutací při skládání Rubikovy kostky (stále odhlížíme od přesné pozice kostiček) je trojcyklus – libovolnou sudou permutaci lze složit z trojcyklů.

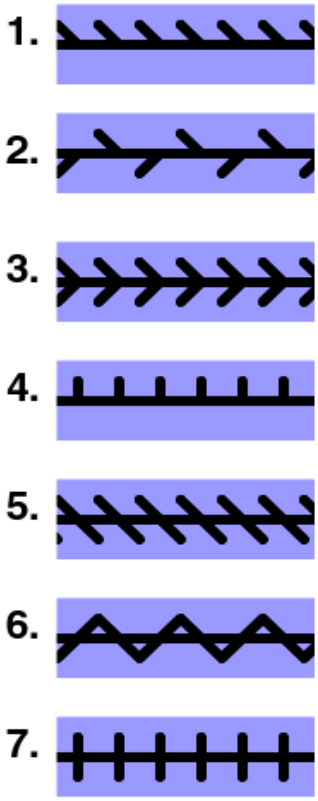
Po nalezení dvou trojcyklů (jednoho pro hranové, jednoho pro rohové kostičky) lze poměrně snadno vytvářet trojcykly další, využívá se při tom konjugovaných permutací, které provádějí „analogické permutace, ovšem mezi jinými kostičkami“.

Umíme již tedy složit Rubikovu kostku, zatím ovšem bez ohledu na orientaci dílčích krychliček. Správného orientování docílíme analogickým postupem – postupujeme zvlášť u rohových a hranových kostiček, nalezneme základní postup pro změnu orientace kostiček a tento postup konjugujeme s vhodnými permutacemi (viz [10]).

5 Krystalografické grupy

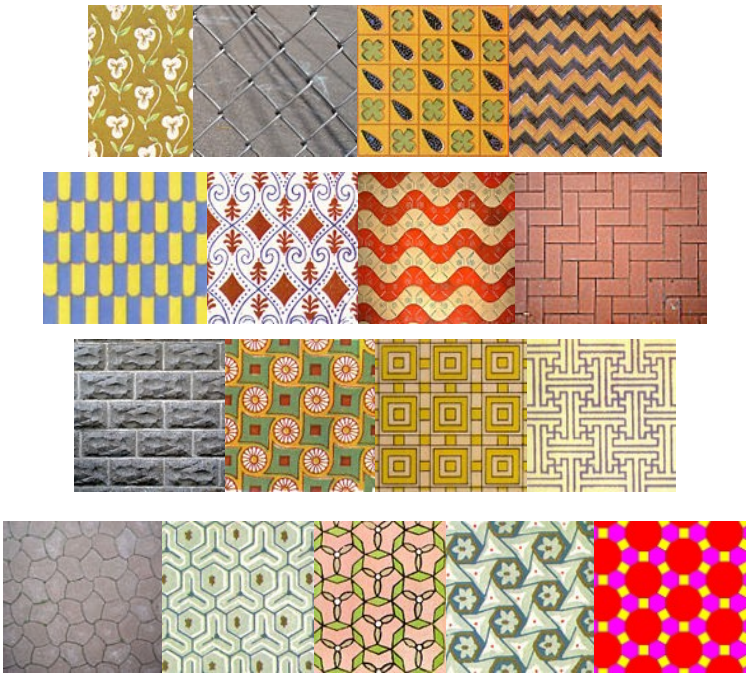
Dříve než se dostaneme ke krystalografickým grupám, uvedeme dvě jednodušší skupiny grup, založené na podobném principu. Uvažujme nejprve vzory v rovině periodicky se opakující v jednom směru s a zkoumejme grupy jejich symetrií, tzv. *Friezovy grupy*. Již z definice je patrné, že tyto grupy budou obsahovat translace o násobek jisté minimální vzdálenosti d ve směru s. Zdůrazněme, že uvažujeme pouze diskrétní grupy (tím vylučujeme např. spojitou grupu symetrií přímky). Existuje 7 různých typů těchto grup, popišme dále jejich symetrie:

1. pouze translace, 2. translace a posunutá zrcadlení, 3. translace, posunutá zrcadlení a osová souměrnost dle osy rovnoběžné se směrem s, 4. translace a osové souměrnosti dle os kolmých na směr s, 5. translace a středové souměrnosti (= otočení o přímý úhel), 6. translace, posunutá zrcadlení, středové souměrnosti a osové souměrnosti dle os kolmých na směr s, 7. translace, posunutá zrcadlení, středové souměrnosti, osové souměrnosti dle os kolmých na směr s, osová souměrnost dle osy rovnoběžné se směrem s (viz [W11]).



Obrázek 4: Friezovy grupy

Uvažujme dále rovinné vzory, periodicky se opakující ve dvou směrech. Existuje 17 různých typů grup symetrií těchto vzorů, zde se spokojíme s uvedením příkladů těchto vzorů.



Obrázek 5: Grupy symetrií, 2D

Rozšířením předchozího konceptu na tři dimenze získáváme již zmiňované krystalografické grupy, grupy symetrií krystalu, kterých existuje celkem 230. Je více způsobů kategorizace těchto grup. Každou z grup lze přiřadit do jedné ze sedmi tzv. *krystalografických soustav* (trojklonná, jednoklonná, kosočtverečná, čtverečná, šesterečná, klencová, krychlová), udávajících vzájemný vztah tří směrů opakování vzorku. Uvažujeme-li i umístění případných „dalších atomů“ ve struktuře krystalu, získáme rozčlenění na 14 tzv. *Bravaisových mřížek.*

6 Jednoduché grupy

Jak jsme již ukázali, má-li grupa normální podgrupu, můžeme ji touto podgrupou „vydělit“, čímž získáme faktorovou grupu grupy podle normální podgrupy. Při této operaci vždy několik prvků vytvoří třídu, prvek faktorové grupy. Pro hrubé přiblížení lze říci, že faktorová grupa je vlastně „pohled z dálky“, kdy nevidíme detaily, pouze hrubou strukturu. Pokud tato možnost „pohledu z dálky“ neexistuje, hovoříme o jednoduché grupě. Jednoduchou grupou tedy rozumíme netriviální grupu, jejíž jedinou normální podgrupou je triviální podgrupa.

Jednoduché grupy jsou jakýmsi základním stavebním blokem teorie grup, r. 1982 byla dokončena klasifikace všech konečných jednoduchých grup.

Nejjednodušším příkladem jednoduché grupy je cyklická grupa prvočíselného řádu – tato grupa nemá žádné netriviální podgrupy, tedy ani netriviální normální podgrupy. Lze ukázat, že cyklické grupy prvočíselného řádu jsou jedinými komutativními jednoduchými grupami.

Nejmenší nekomutativní jednoduchou grupou je grupa A_5 řádu 60.

Každá jednoduchá grupa náleží minimálně do jedné z následujících tříd:

- cyklická grupa prvočíselného řádu
- alternující grupa stupně alespoň 5
- grupa Lieova typu
- sporadická grupa

Nejzajímavější z těchto skupin jsou bezesporu sporadické grupy – jedná se o 26 grup, které nepatří do žádné z předchozích kategorií. Až na 6 z nich jsou všechny obsaženy v největší sporadické grupě, která se nazývá *Monster group* a je řádu přibližně $8 \cdot 10^{53}$.

Zajímavou knihou, zabývající se strukturou jednoduchých grup je kniha [12]. Slovu „atlas“ v názvu odpovídá i formát této knihy – A3. Zachycuje mj. popisy nekomutativních jednoduchých grup, počínaje již zmiňovanou grupou A_5 a konče patnáctistránkovým popisem *Monster group*. V jednotlivých kategoriích postupovali autoři v popisu tak dlouho, než začaly být grupy příliš komplikované či nudné. Lze souhlasit s jejich tvrzením: „*In doubtful cases, our rule was to think how far the reasonable person would go, and then go a step further“*. V tomto atlase nejsou z pochopitelných důvodů uvedeny Cayleyho tabulky, ale informace typu řád grupy, různé způsoby konstrukce, maximální podgrupy atd.

Seznam pramenů

[1] Zassenhaus H., *The theory of groups*, Chelsea Publishing Company, New York, 1949.
[2] Alexandrov P. S., *Úvod do teorie grup*, Mir, Moskva, 1985.
[3] Bican L., *Algebra (pro učitelské studium)*, Academia, Praha, 2001.
[4] Bečvář J., *Lineární algebra*, Matfyzpress, Praha, 2000.
[5] Beran L., *Grupy a svazy*, SNTL, Praha, 1974.
[6] Hall M. J., *Theory of Groups*, American Mathematical Society, Providence, 1999.
[7] Rieger L., O *grupách a svazech*, Přírodovědecké vydavatelství, Praha, 1952.
[8] Kurosh A. G., *The Theory of Groups, Volume One*, American Mathematical Society, Providence, 2003.
[9] Kurosh A. G., *The Theory of Groups, Volume Two*, American Mathematical Society, Providence, 2003.
[10] Tůma J., *Matematické hlavolamy*, Mladá fronta, Praha, 1988
[11] Trkovská D., *Erlangenský program*, publikováno ve sborníku *Dějiny matematiky, svazek 33, Matematika v proměnách věků V*, editoři Bečvářová M., Bečvář J., Matfyzpress, Praha, 2007.
[12] Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A., *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[W1] Kolektiv autorů, *Introduction to Group Theory*, nedatováno, http://members.tripod.com/~dogschool/index.html, (18. 2. 2008).
[W2] Kolektiv autorů, *Wikipedia, the free encyclopedia*, nedatováno, http://en.wikipedia.org/wiki/Homomorphism, (18. 2. 2008).
[W3] Kolektiv autorů, *Physics Forums*, nedatováno, http://www.physicsforums.com/showthread.php?page=21&t=122924, (27. 3. 2008).
[W4] Taylor G., *Groups of order 2p*, nedatováno, http://tartarus.org/gareth/maths/Groups/groups_order_2p.pdf, (27. 3. 2008).
[W5] Kolektiv autorů: *Wikipedia, the free encyclopedia*, nedatováno, http://en.wikipedia.org/wiki/Dihedral_group, (18. 2. 2008).
[W6] Kahrobaei D., *Groups of small orders*, nedatováno, http://www-groups.mcs.st-andrews.ac.uk/~delaram/Groups/small.pdf, (27. 3. 2008).
[W7] Lynn B., *Group theory*, nedatováno, http://crypto.stanford.edu/pbc/notes/group/ordereight.xhtml, (27. 3. 2008).
[W8] Joyner D., *The second and third Sylow Theorems*, 12. 4. 2001, http://web.usna.navy.mil/~wdj/tonybook/gpthry/node56.html, (27. 3. 2008).
[W9] Kolektiv autorů, *Wikipedia, the free encyclopedia*, nedatováno, http://en.wikipedia.org/wiki/List_of_small_groups, (27. 3. 2008).
[W10] Zahradník M., Motl L., *Pěstujeme lineární algebru*, 23. 11. 1997, http://www.kolej.mff.cuni.cz/~lmotm275/skripta/mzahrad/node20.html, (27. 3. 2008).
[W11] Kolektiv autorů, *Wikipedia, the free encyclopedia*, nedatováno, http://en.wikipedia.org/wiki/Frieze_group, (27. 3. 2008).

Seznam tabulek

Seznam obrázků