

02GR - Odmaturuj z Grup a Reprezentací

podle přednášky doc. Ing. Goce Chadzitaskose, CSc

21. srpna 2021

Obsah

1	Grupy	4
1.1	Algebraický koncept	4
1.2	Vlastnosti grup	6
1.3	Homomorfismus a isomorfismus grup	8
2	Podgrupy	9
2.1	Centralizátory a normalizátory	9
2.2	Cyklické grupy	10
2.3	Svazy podgrup	11
2.3.1	Hasseovy diagramy	12
3	Faktor grupy	14
3.1	Levé a pravé třídy	15
3.2	Normální podgrupy	17
3.3	Index grupy, Lagrangeova věta	18
3.4	Součinná podgrupa	19
3.5	Věty o isomorfismech	20
3.6	Kompoziční řady	22
4	Akce grupy na množině	24
4.1	Stabilizátory a orbity	24
4.2	Rovnice tříd	26
5	Sylowova věta	28
6	Přímý a polopřímý součin grup	31
6.1	Klasifikace Abelovských grup	31
6.2	Polopřímý součin	33
7	Reprezentace grup	35
7.1	Základní definice	35
7.2	Reducibilní a ireducibilní reprezentace	36
7.2.1	Schurova lemmata	37
7.3	Velká věta ortogonality	38
7.4	Tabulky charakterů	39
	Literatura	41

Předmluva

Toto wikiskriptum vzniklo podle přednášek prof. Ing. Goce Chadzitaskose, CSc. k předmětu Grupy a Reprezentace vyučovaného pro 1. ročník navazujícího magisterského studia na FJFI ČVUT v Praze v zimním semestru roku 2012. Z velké části však jen podle učebnice [1], proto by bylo potřeba ho dodělat a sjednotit s přednáškou.

V zimním semestru roku 2015 došlo k první velké úpravě tohoto wikiskripta, mnoho bylo doplněno a opraveno a jednotlivé části byly seřazeny podle letošní přednášky. Stále však není wikiskriptum kompletní, je třeba doplnit zejména **poslední kapitolu o reprezentacích** a pár dalších důkazů. Případné chyby je třeba opravit. Prosíme tedy posluchače toho předmětu, aby se chopili úprav tohoto wikiskripta, aby existoval nějaký uspořádaný a spolehlivý doplněk k jinak neuspořádané přednášce. :-)

1 Grupy

1.1 Algebraický koncept

Definice 1.1. Mějme libovolnou množinu M . Potom **n-ární operací** na M nazveme zobrazení $f : M \times M \times \dots \times M \rightarrow M$.

Definice 1.2. Operaci $f : M \times M \rightarrow M$ (binární operace) budeme nazývat **vnitřní součin** a místo $f(x, y) = z$ ji budeme značit $xy = z$.

POZNÁMKA 1.3. Neplést vnitřní součin s pojmem skalární součin (angl.: scalar product = inner product). Příkladem binární operace na vektorovém prostoru je vektorový součin vektorů.

Definice 1.4. Dvojici $\{M, \cdot\}$ nazýváme **grupoid**. Dále při splnění dodatečných podmínek zavádíme:

1. $(\forall a, b, c \in M)((ab)c = a(bc))$: **pologrupa** (asociativní grupoid),
2. $(\forall a, b \in M)(ab = ba)$: **komutativní grupoid**,
3. počet prvků M je konečný: **konečný grupoid**.

Definice 1.5. Levou resp. pravou **jednotkou** v grupoidu nazýváme takový prvek e , pro který platí $eg = g$ respektive $ge = g$ pro každé g z grupoidu.

Věta 1.6. *Má-li grupoid levou a pravou jednotku, pak jsou stejné.*

Důkaz. $e_l = e_l e_p = e_p$ □

Definice 1.7. Pologrupu s jednotkovým prvkem nazýváme **monoid**. Navíc pokud pro $m \in M$ existuje $m^{-1} \in M$ takový, že $m^{-1}m = e$ resp. $mm^{-1} = e$, nazýváme m^{-1} **levým, resp. pravým inverzním** prvkem k m . (Díky asociativitě platí rovnost mezi levým a pravým inverzním prvkem, protože pro levou inverzi $am = e$ a pravou inverzi $mb = e$ platí $b = eb = (am)b = a(mb) = ae = a$. Proto má smysl zavést značení m^{-1} .)

Věta 1.8. *Každý prvek monoidu má nejvýše jeden inverzní prvek.*

Důkaz. Necht' $f, g, m \in M$ a platí $fm = e$ a $gm = e$, pak $f = ef = gm f = ge = g$. V předposledním rovnítku využíváme asociativitu. □

Definice 1.9. Zavádíme:

1. grupoid s **krácením**, pokud $(\forall x, y, z \in M)(zx = zy \Rightarrow x = y)$,
2. grupoid s **dělením**, pokud $(\forall x, y \in M)(\exists u, v \in M)(ux = xv = y)$.

1 Grupy

Definice 1.10. Monoid, ve kterém ke každému prvku existuje inverzní prvek nazýváme **grupa**.

POZNÁMKA 1.11. Grupa $\{M, \cdot\}$ tedy splňuje vlastnosti:

1. $(\forall a, b, c \in M)((ab)c = a(bc)),$
2. $(\exists e \in M)(\forall m \in M)(em = m),$
3. $(\forall m \in M)(\exists m^{-1} \in M)(mm^{-1} = e).$

PŘÍKLAD 1.12. Příkladem grupy může být:

1. množina regulárních matic rozměru $n \times n$ s maticovým násobením,
2. množina čísel $\{0, 1, 2, \dots, p-2, p-1\}$ se sčítáním modulo p pro nějaké prvočíslo p , tedy $a \oplus_{\text{modulop}} b \equiv a + b \pmod{p}$, (značená $\mathbb{Z}_p \equiv \mathbb{Z}/p\mathbb{Z}$),
3. množina kvaternionů s násobením.

Definice 1.13. Komutativní grupu nazýváme **abelovská**.

Definice 1.14. Mějme množinu se dvěma vnitřními součiny $\{M, \oplus, \odot\}$.

1. Pokud je M Abellovská grupa vůči $\oplus$ a pologrupa s distributivním zákonem vůči $\odot$ (tedy $a \odot (b \oplus c) = ab \oplus ac$), nazýváme ji **okruh**.
2. Pokud je M Abellovská grupa vůči $\oplus$ a $M \setminus \{0\}$ grupa vůči $\odot$, nazýváme M **okruh s dělením**.
3. Pokud je M Abellovská grupa vůči $\oplus$ a $M \setminus \{0\}$ Abellovská grupa vůči $\odot$, nazýváme M **těleso**.

POZNÁMKA 1.15. Značku 0 používáme pro jednotkový prvek vůči operaci značené $\oplus$ a značku 1 pro jednotkový prvek vůči operaci značené $\odot$ nebo $\otimes$.

PŘÍKLAD 1.16. Dalším příkladem grupy je množina $\mathbb{Q}[\sqrt{p}] = \{m + n\sqrt{p} | m, n \in \mathbb{Q}\}$ s normálním násobením, kde $\mathbb{Q}$ jsou racionální čísla a p je prvočíslo. (Odmocnina z prvočísla je vždy iracionální.) Jedná se o určitou analogii komplexních čísel: $a \cdot b = (a_1 + a_2\sqrt{p})(b_1 + b_2\sqrt{p}) = a_1b_1 + a_2b_1\sqrt{p} + a_1b_2\sqrt{p} + a_2b_2p$.

Definice 1.17. Mějme množinu M , těleso $\mathbb{T}$, vnitřní součin $+: M \times M \rightarrow M$ a vnější součin $\times: \mathbb{T} \times M \rightarrow M$. Čtveřici $\{M, \mathbb{T}, +, \times\}$ nazýváme **vektorový prostor**, pokud je abelovskou grupou vůči $+$ a platí:

1. $(\forall \alpha \in \mathbb{T})(\forall x, y \in M)(\alpha \times (x + y) = \alpha \times x + \alpha \times y),$
2. $(\forall \alpha, \beta \in \mathbb{T})(\forall x \in M)((\alpha + \beta) \times x = \alpha \times x + \beta \times x),$
3. $(\forall x \in M)(1 \times x = x),$
4. $(\forall x \in M)(0 \times x = 0).$

Definice 1.18. Mějme $\{M, \mathbb{T}, +, \times, \odot\}$ vektorový prostor s dodatečným vnitřním součinem $\odot$. Zavádíme pojmy:

1 Grupy

1. pro M grupoid s distributivním zákonem vůči $\odot$ **lineární algebra** nad $\mathbb{T}$,
2. pro M pologrupu s distributivním zákonem vůči $\odot$ **asociativní algebra** nad $\mathbb{T}$,
3. pro M pologrupu s distributivním a komutativním zákonem vůči $\odot$ **komutativní algebra** nad $\mathbb{T}$.

1.2 Vlastnosti grup

Jednou z možností je klasifikace grup podle počtu prvků na konečné, diskrétní nekonečné (spočetné), nespočetné.

Definice 1.19. Mějme grupu $G = \{M, \cdot\}$ a topologii na M . G nazýváme **topologickou grupou**, pokud pro $\forall x, y \in M$ jsou zobrazení $f_y(x) = x \cdot y$ a $g(x) = x^{-1}$ spojitá.

PŘÍKLAD 1.20. Mějme grupu $G = \{\{e, a, b\}, \odot\} \equiv \mathbb{Z}_3 = \{\{0, 1, 2\}, +_{mod3}\}$. Její strukturu můžeme zobrazit pomocí tabulky.

$\odot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

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

Pokud zvolíme topologii $\tau = \{\emptyset, e, a, \{e, a\}, G\}$, nedostaneme topologickou grupu, protože vzor otevřené množiny $\{a\}$ při zobrazení $g(x) = x^{-1}$ je množina $\{b\}$, která není otevřená.

Definice 1.21. Topologický prostor $\{M, \{\nu_i\}\}$ nazýváme **homogenní**, pokud $(\forall x, y \in M)$ existuje homeomorfismus (spojitá bijekce se spojitou inverzí) takový, že $f(x) = y$.

Věta 1.22. Každá topologická grupa je homogenní topologický prostor.

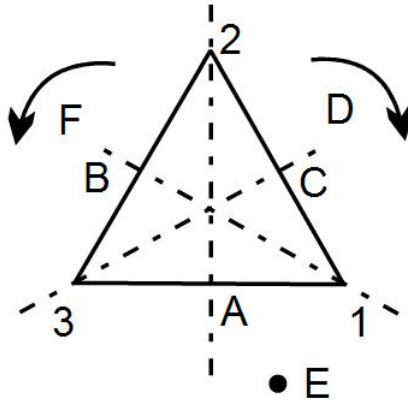
Důkaz. Mějme $x, y \in G$ a nechť $a = yx^{-1}$. Určitě platí $a \in G$ a $ax = yx^{-1}x = y$. Hledaný homeomorfismus tedy bude $f(x) = ax$ (spojitost operací v topologické grupě). $\square$

POZNÁMKA 1.23. Topologická grupa má lokální vlastnosti $\mathbb{R}^n$.

Definice 1.24. Topologickou grupu G nazýváme **n -parametrická**, pokud:

1. $(\exists \text{ systém souřadnic } \{\varphi\} \text{ v } G)(\varphi : G \rightarrow \mathbb{R}^n : x \rightarrow (\alpha_1, \alpha_2, \dots, \alpha_n))$,
2. φ může být i pouze lokální, ale pro každé dva souřadné systémy φ, ψ musí být $\varphi \circ \psi^{-1}$ spojitý (tam, kde je definován),
3. souřadnice bodu $c = a \cdot b$ jsou spojitou funkcí a a b .

PŘÍKLAD 1.25. Grupa $G = GL(n, \mathbb{R})$ je množina všech nesingulárních ($\det \neq 0$) reálných matic rozměru $n \times n$. Zavedeme n^2 souřadnic tak, že prvku $x \in G$, kde $x = \mathbb{I} + \tilde{x}$ ($\mathbb{I}$ je jednotková matice), přiřadíme prvky matice $\tilde{x}$, tedy $\{x_{i,j}\}_{i,j=1}^n$.

Obrázek 1.1: Zobrazení grupy D_6 .

POZNÁMKA 1.26. I u grupového násobení používáme mocniny jako u násobení čísel, tedy pro $g \in G$ píšeme g^n místo $g \cdot g \cdot \dots \cdot g$ (n -krát).

Definice 1.27. Řád prvku a v grupě G je číslo n , pro které platí $(a^n = e) \wedge ((\forall m < n)(a^m \neq e))$. (Tedy nejmenší mocnina a , která dá jednotku.)

Definice 1.28. Řád grupy je počet jejích prvků (značíme $|G|$).

POZNÁMKA 1.29. Pro každý $g \in G$ platí $|g| \leq |G|$. Pro nekonečný řád grupy to platí triviálně, pro konečnou grupu platí následující argument: Vezměme posloupnost $\{g^n\}_{n \in \mathbb{N}}$ pro libovolný prvek $g \in G$. Každý prvek posloupnosti je prvkem G (uzavřenost na násobení). Protože G má konečný počet prvků, pak jistě existují indexy n_1, n_2 tak, že $g^{n_1} = g^{n_2}$. Z toho ale plyne $g^{n_1 - n_2} = e$, tedy g má konečný řád. Kdyby existoval prvek s řádem $n > |G|$, pak by posloupnost $\{g^i\}_{i=0}^{n-1}$ měla n různých prvků, tj. více než kolik jich je v G , což je spor, tudíž $n \leq |G|$.

Definice 1.30. Generátory grupy jsou prvky minimálního souboru (s minimálním počtem prvků), ze kterého je možné získat celou grupu pomocí vzájemného násobení. Počet generátorů nazýváme **rank** grupy ($\text{Rank}(G)$).

PŘÍKLAD 1.31. Dihedrál ní grupa D_6 je grupa symetrií rovnostranného trojúhelníku, viz Obr. 1.1.

$\odot$	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	E	D	F	B	C
B	B	F	E	D	C	A
C	C	D	F	E	A	B
D	D	C	A	B	F	E
F	F	B	C	A	E	D

Pravidla pro násobení je možné popsat vztahy $A^2 = E$, $D^3 = E$, $DA = AD^2 (= AD^{-1})$. Generátory jsou například $\{A, D\}$, a tedy $\text{Rank}(D_6) = 2$.

1 Grupy

PŘÍKLAD 1.32. Dihedrál ní grupa D_{2n} představující symetrie pravidelného n -úhelníku (n rotací a n zrcadlení). Generátory grupy jsou r (rotace o nejmenší úhel) a s (libovolné zrcadlení). Násobení je zavedeno pomocí vztahů $r^n = e$, $s^2 = e$, $rs = sr^{-1}$.

PŘÍKLAD 1.33. Cyklická grupa $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ se sčítáním modulo n . Grupa je generována například prvkem 1 (v této grupě číslo 1 není jednotkový prvek, to je 0) ($\text{Rank}(\mathbb{Z}_n) = 1$). Ekvivalentně je možno tuto grupu zavést jako množinu $\{e^{i\frac{2\pi}{n}k}\}_{k=0}^{n-1}$ s násobením.

PŘÍKLAD 1.34. Symetrická grupa S_Ω na množině $\Omega \neq \emptyset$ je grupa permutací prvků množiny Ω . Tedy S_Ω představuje všechny bijekce na Ω a v případě $\Omega = \hat{n}$ platí $|S_n| = n!$.

PŘÍKLAD 1.35. Grupa kvaternionů $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ s relacemi $i^2 = j^2 = k^2 = ijk = -1$.

1.3 Homomorfismus a isomorfismus grup

Definice 1.36. Grupy $\{G, \cdot\}$ a $\{H, \times\}$ jsou **homomorfní**, když $(\exists \varphi : G \rightarrow H)(\forall x, y \in G)(\varphi(x \cdot y) = \varphi(x) \times \varphi(y))$. Zobrazení φ se nazývá **homomorfismus**, popř.

- **monomorfismus**, je-li prosté,
- **epimorfismus**, je-li na H ,
- **isomorfismus**, je-li bijekcí (prosté i na H),
- **endomorfismus**, je-li $G = H$ (tj. zobrazuje do sebe),
- **automorfismus**, je-li $G = H$ a isomorfní (tj. zobrazuje na sebe),

Dále definujeme **jádro** homomorfismu: $\text{Ker } \varphi = \{x \in G \mid \varphi(x) = e_H\}$.

- tvoří grupu $\text{Aut}(G)$

POZNÁMKA 1.37. Neplést homomorfismus (zobrazení zachovávající algebraickou strukturu) a homeomorfismus (spojité zobrazení se spojitou inverzí)!

PŘÍKLAD 1.38. Grupy $GL(n, \mathbb{R})$ (nesingulární reálné matice) a $G = \{\mathbb{R}^+, \cdot\}$ (kladná reálná čísla s násobením) jsou homomorfní pomocí zobrazení $\varphi(A) = \det A$.

PŘÍKLAD 1.39. Grupa $(\mathbb{R}, +)$ je izomorfní grupě $(\mathbb{R}^+, \cdot)$ přes zobrazení $\varphi(x) = e^x$, jelikož platí $e^x \cdot e^y = e^{x+y}$.

PŘÍKLAD 1.40. Pro libovolnou grupu G je zobrazení $\varphi : G \rightarrow G$ definované pro $\forall f \in G$ jako $\varphi(f) = gfg^{-1}$ (pro $g \in G$ pevné) automorfismus, tj. $\varphi \in \text{Aut } H$.

POZNÁMKA 1.41. Nutné podmínky pro to, aby $\varphi : G \rightarrow H$ mohlo být isomorfismus:

1. $|G| = |H|$,
2. G je abelovská právě tehdy, když H je abelovská,
3. $(\forall x \in H)(|\varphi(x)| = |x|)$.

2 Podgrupy

Definice 2.1. Neprázdná podmnožina H grupy G , tj. $\emptyset \neq H \subset G$, je **podgrupa** grupy G (značíme $H \leq G$), pokud je grupou vůči násobení v G . (Tedy obsahuje jednotku z G a je uzavřená vůči násobení prvků z H a jejich inverzi.)

PŘÍKLAD 2.2. Množina $\{E, A\}$ je podgrupou v D_6 ($A^2 = E$, $A^{-1} = A$).

Věta 2.3. Množina $\emptyset \neq H \subset G$ je podgrupa $\Leftrightarrow (\forall x, y \in H)(xy^{-1} \in H)$.

Důkaz. Implikace $\Rightarrow$ plyne přímo z definice podgrupy. Dokážeme opačnou implikaci. Z definice je H neprázdná, a tedy můžeme vzít $g \in H$. Pokud nyní položíme $x = g$ a $y = g$, máme $gg^{-1} \in H$, tedy H obsahuje jednotku. Dále tedy volíme $x = 1$ a $y = g$ a dostáváme $1g^{-1} \in H$, tedy H obsahuje inverzi g . Nakonec pro libovolné prvky $f, g \in G$ volíme $x = f$ a $y = g^{-1}$, dostáváme $f(g^{-1})^{-1} \in H$, tedy H obsahuje součin fg . $\square$

POZNÁMKA 2.4. Pro konečnou podgrupu $H \leq G$ platí $(\forall x \in H)(|x| < \infty)$.

2.1 Centralizátory a normalizátory

Definice 2.5. Bud' $\emptyset \neq A \subset G$. Definujeme **centralizátor** množiny A v G jako: $C_G(A) = \{g \in G | gag^{-1} = a \text{ pro } \forall a \in A\}$.

POZNÁMKA 2.6. Jelikož $(gag^{-1} = a) \Leftrightarrow (ga = ag)$, je centralizátor množiny A množina všech prvků z G , které komutují se všemi prvky z A .

Věta 2.7. Množina $C_G(A)$ je podgrupa v G .

Důkaz. Víme, že $C_G(A)$ je neprázdná, jelikož $1 \in C_G(A)$ (z definice komutuje se vším). Dále mějme $x \in C_G(A)$. Pak pro $\forall a \in A$ platí:

$$\begin{aligned} x^{-1} | \quad xax^{-1} &= a \quad |x \\ a &= x^{-1}ax, \end{aligned}$$

tedy $x^{-1} \in C_G(A)$. Pro dva prvky $x, y \in C_G(A)$ pak máme:

$$(xy)a(xy)^{-1} = x(yay^{-1})x^{-1} = xax^{-1} = a,$$

a tedy centralizátor je uzavřený i vůči násobení. $\square$

Definice 2.8. Definujeme **centrum** grupy G jako: $Z(G) = \{g \in G | gfg^{-1} = f \text{ pro } \forall f \in G\}$.

POZNÁMKA 2.9. Platí, že $Z(G) = C_G(G)$, tedy je to množina prvků G , které komutují se všemi ostatními. Jako speciální případ předchozí věty platí $Z(G) \leq G$.

2 Podgrupy

Definice 2.10. Pro $A \subset G$ a $g \in G$ zavádíme značení: $gA = \{ga | a \in A\}$. Obdobně pro Ag , a tedy konkrétně $gAg^{-1} = \{gag^{-1} | a \in A\}$.

Definice 2.11. Buď $\emptyset \neq A \subset G$. Definujeme **normalizátor** A v G jako: $N_G(A) = \{g \in G | gAg^{-1} = A\}$.

POZNÁMKA 2.12. Normalizátor se od centralizátoru liší tím, že může prvky A zpermutovat (množina A se tím nezmění). Grupové vlastnosti $N_G(A)$ se ukáží podobně jako u $C_G(A)$.

Tvrzení 2.13. Platí, že $C_G(A) \leq N_G(A) \leq G$.

Důkaz. $N_G(A) \leq G$: Použijeme značení z def. 2.10.

1. $N_G(A) \neq \emptyset$, protože $e \in N_G(A)$.
2. Necht' $x, y \in N_G(A)$, tj. $xAx^{-1} = A$ a $yAy^{-1} = A$. Pak platí $(xy)A(xy)^{-1} = x \underbrace{(yAy^{-1})}_A x^{-1} = xAx^{-1} = A$. (Asociativita platí z vlastností grupového násobení v G .) To ale znamená, že $(xy) \in N_G(A)$.
3. Necht' $x \in N_G(A)$. Pak zřejmě platí $xAx^{-1} = A \Rightarrow x^{-1}Ax = A$, tj. $x^{-1} \in N_G(A)$, čímž je $N_G(A) \leq G$ dokázáno.

$C_G(A) \leq G$ již bylo dokázáno a $C_G(A) \leq N_G(A)$ je pak zřejmé z definice podgrupy. □

2.2 Cyklické grupy

Definice 2.14. Grupu nazýváme **cyklická**, pokud je generována jen jedním prvkem a a značíme $H = \langle a \rangle = \{a^n | n \in \mathbb{Z}, a^0 = e\}$.

POZNÁMKA 2.15. Cyklická grupa je vždy abelovská (komutativní).

POZNÁMKA 2.16. Dvě cyklické grupy $\langle x \rangle$ a $\langle \xi \rangle$ stejného řádu jsou isomorfní ($\varphi(x^n) = \xi^n$).

Věta 2.17. Pro grupu $G = \langle x \rangle$ platí $|G| = |x|$.

Důkaz. 1. Pro $|x| = \infty$ jsou všechny prvky c^α různé pro $\forall \alpha \in \mathbb{N}$, tedy jich je nekonečně mnoho.

2. Necht' $|x| = n$. Platí $(\forall \alpha \in \mathbb{Z})(\alpha = kn + m)$, pro nějaké $n \in \mathbb{Z}$ a $(m \in \mathbb{Z}^+)(m \leq n)$. Potom $s^\alpha = x^{kn}x^m = ex^m$. Máme tedy právě n prvků v G . □

POZNÁMKA 2.18. Největší společný dělitel čísel n a m značíme $\gcd(n, m)$.

Věta 2.19. Mějme grupu $G = \langle x \rangle$. Potom platí:

1. $|G| = \infty \Rightarrow |x^\alpha| = \infty$ a navíc $(x^\alpha \neq x^\beta)(\forall \alpha, \beta \in \mathbb{Z} \setminus \{0\})$,
2. $|G| = n \Rightarrow |x^\alpha| = \frac{n}{\gcd(n, \alpha)}$ pro $\alpha \in \mathbb{Z} \setminus \{0\}$.

2 Podgrupy

Důkaz. 1) $|G| = \infty$ znamená, že $|x| = \infty$, tedy $(\forall a \in \mathbb{N})((x^a)^n = x^{na} \neq e)$. Důkaz druhé části provedeme sporem, tedy necht' $x^\alpha = x^\beta$. Potom $x^{\alpha-\beta} = x^0 = 1$ (tedy $|x| = \alpha - \beta$), což je spor.

2) Víme tedy, že $|x| = n$. Označme si $d = \gcd(n, \alpha)$. Musí existovat celé číslo c takové, že $\alpha = cd$. Jelikož α i n jsou pevná, pak i c je pevně určeno. Nyní budeme hledat nejmenší $a \in \mathbb{N}$ takové, aby $(x^\alpha)^a = x^{\alpha a} = e$. Musí tedy platit $\alpha a = bn$ pro nějaké $b \in \mathbb{N}$, které si můžeme volit. To dále upravíme:

$$\begin{aligned}\alpha a &= bn \\ cda &= bn \\ a &= \frac{bn}{cd}.\end{aligned}$$

Víme, že $\frac{n}{d}$ je celé číslo. Jelikož a musí být také celé číslo a navíc chceme, nejmenší možné, zvolíme $b = c$. Nemůžeme volit $b < c$, protože aby pak bylo a celé, muselo by mít c a n společného dělitele, což je spor s definicí c . Tím dostáváme tvrzení věty. (Doporučuji si to vyzkoušet na konkrétních číslech, třeba $n = 4$ a $\alpha = 6$.) $\square$

POZNÁMKA 2.20. Každá podgrupa grupy $\langle x \rangle$ je cyklická.

Definice 2.21. Podgrupa **generovaná podmnožinou** $M \subset G$ je nejmenší podgrupa G obsahující všechny prvky M . Tedy

$$\langle M \rangle = \bigcap_{\substack{H_i \leq G \\ M \subset H_i}} H_i.$$

$$A = \{a_1, \dots, a_n\}$$

$$\bar{A} = \{a_{i_1}^{\varepsilon_{i_1}} \cdot a_{i_2}^{\varepsilon_{i_2}} \cdot \dots \cdot a_{i_k}^{\varepsilon_{i_k}}\}$$

a_{i_j} se může opakovat

POZNÁMKA 2.22. Snadno se ukáže, že průnik dvou podgrup je opět podgrupa.

$$\varepsilon_{i_j} = \pm 1$$

2.3 Svazy podgrup

$$\langle A \rangle = \bar{A}$$

Nyní zavedeme relaci uspořádání, abychom mohli zavést svazy podgrup a kreslit tzv. Hasseho diagramy.

Definice 2.23. Relaci $\preceq$ na množině M nazýváme **částečné uspořádání**, pokud platí:

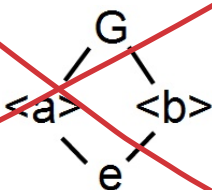
1. reflexivita: $(\forall x \in M)(x \preceq x)$,
2. tranzitivita: $(\forall x, y, z \in M)(x \preceq y \wedge y \preceq z \Rightarrow x \preceq z)$,
3. slabá antisymetrie: $(\forall x, y \in M)(x \preceq y \wedge y \preceq x \Rightarrow x = y)$.

PŘÍKLAD 2.24. Mějme libovolnou množinu A a její potenční množinu $\mathcal{P}(A) = 2^A$. Zavedeme uspořádání $(\forall M, N \in 2^A)(M \preceq N \Leftrightarrow M \subset N)$.

PŘÍKLAD 2.25. Grupa $G = \{e, a, b | a^2 = e, b^2 = e\}$ má podgrupy $\{e\}$, $\langle a \rangle$, $\langle b \rangle$ a G . Můžeme zavést uspořádání pomocí relace "být podgrupou", tedy způsobem: $G_1 \preceq G_2 \Leftrightarrow G_1 \leq G_2$. Obr. 2.1.

Definice 2.26. Buď $\{M, \preceq\}$ množina s částečným uspořádáním a $A \subset M$ její podmnožina. Prvek $x \in M$ nazveme

2 Podgrupy



taková grupa ~~ž~~!

Obrázek 2.1: Uspořádání na $G = \{e, a, b \mid a^2 = e, b^2 = e\}$ podle relace „být podgrupou“.

- **horní závora** množiny A , pokud $(\forall a \in A)(a \preceq x)$,
- **dolní závora** množiny A , pokud $(\forall a \in A)(x \preceq a)$,
- **supremum** množiny A ($x = \sup_{\preceq} A$), je-li x nejmenší prvek množiny horních závor A ,
- **infimum** množiny A ($x = \inf_{\preceq} A$), je-li x největší prvek množiny dolních závor A .

Definice 2.27. Bud' $\{M, \preceq\}$ množina s částečným uspořádáním. Pak $\forall x, y \in M$ definujeme operace

- **spojení** $x \vee y = \sup_{\preceq} \{x, y\}$.
- **průsek** $x \wedge y = \inf_{\preceq} \{x, y\}$,

POZNÁMKA 2.28. Neplést spojení a průsek ($\vee, \wedge$) s operacemi sjednocení a průnik ($\cup, \cap$).

Definice 2.29. Bud' $\{M, \preceq\}$ množina s částečným uspořádáním a operacemi $\wedge, \vee$. Potom $\{M, \wedge, \vee\}$ nazýváme **svaz**, pokud $(\forall x, y \in M)((x \vee y \in M) \text{ a zároveň } (x \wedge y \in M))$.

Definice 2.30. Svaz $\{M, \wedge, \vee\}$ nazýváme **modulární**, pokud $(\forall a, b, c \in M)((a \preceq c) \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee c)$.

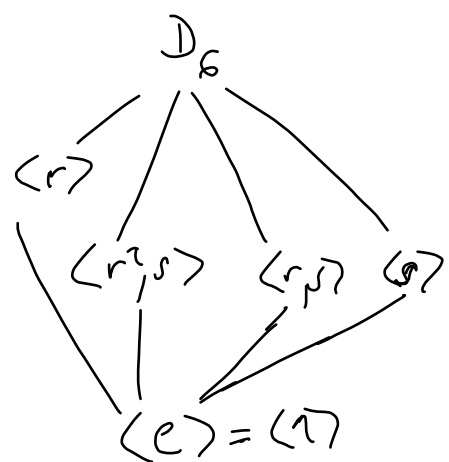
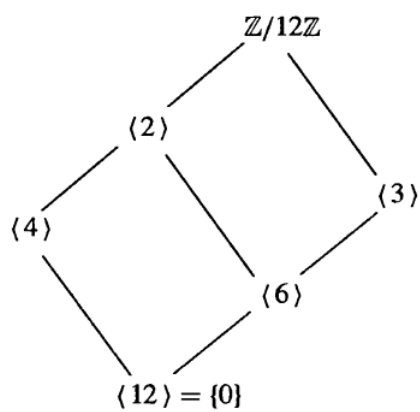
2.3.1 Hasseovy diagramy

Konstrukce **Hasseova diagramu** podgrup konečné grupy G :

POZNÁMKA 2.31. Najdeme všechny podgrupy G a seřadíme je podle jejich řádu. Grupu G umístíme nejvýše a grupu 1 nejniže. Zbytek podgrup rozmístíme podle jejich řádu a čarami spojíme všechny grupy A a B , pro něž $A \leq B$ a neexistuje podgrupa C , pro kterou $C < B$ (vlastní podgrupa) a zároveň $A < C$. (Tedy spojujeme jen „nejbližší“ podgrupy.)

POZNÁMKA 2.32. Mezi každými dvěma podgrupami $A \leq B$ existuje spojnice, ale může vést přes celý řetězec podgrup a těchto spojnic může být i více. Příklad je na Obr. 2.2.

2 Podgrupy

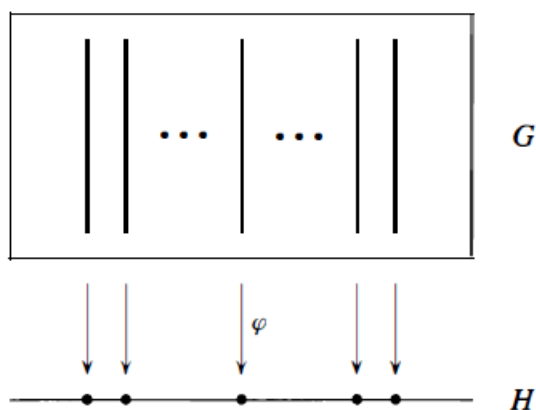


Obrázek 2.2: Svaz podgrup grupy $\mathbb{Z}/12\mathbb{Z}$. Převzato z [1].

3 Faktor grupy

POZNÁMKA 3.1. Studium faktor grup dané grupy G nám umožňuje zkoumat její strukturu a je ekvivalentní zkoumání homomorfismů G .

Definice 3.2. Mějme homomorfismus $\varphi : G \rightarrow H$. **Vláknem** homomorfismu φ příslušejícím prvku $x \in H$ nazýváme množinu $\{y \in G | \varphi(y) = x\}$, tedy množina všech prvků, které se zobrazí na x . (Obr. 3.1).



Obrázek 3.1: Znázornění vláken homomorfismu. Převzato z [1].

Tvrzení 3.3. Pro homomorfismus $\varphi : G \rightarrow H$ platí:

1. $\varphi(e_G) = e_H$
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$
3. $\varphi(g^n) = \varphi(g)^n$
4. $\text{Ker } \varphi \leq G$
5. $\varphi(G) \leq H$

Důkaz. $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G) \varphi(e_G) \implies$ (krácení v H) $\varphi(e_G) = e_H$.

2. $\varphi(g) \varphi(g^{-1}) = \varphi(g g^{-1}) = \varphi(e_G) = e_H$, tedy $\varphi(g^{-1}) = \varphi(g)^{-1}$.

3. Indukcí na n .

4. Stačí dokázat $g_1, g_2 \in \text{Ker } \varphi \implies g_1 g_2^{-1} \in \text{Ker } \varphi$. platí $e_G \in \text{Ker } \varphi$, tj. jádro je neprázdné. Necht' $g_1, g_2 \in \text{Ker } \varphi$. Pak $\varphi(g_1) = \varphi(g_2) = e_G$. Potom $\varphi(g_1 g_2^{-1}) = \varphi(g_1) \varphi(g_2^{-1}) = e_H$.

5. Stejně jako předchozí bod, jen předpoklad $h_1 = \varphi(g_1)$. □

3 Faktor grupy

Definice 3.4. Mějme homomorfismus $\varphi : G \rightarrow H$ s jádrem $\text{Ker } \varphi = K$. Potom **faktor grupa** G/K ($G \text{ mod } K$) je grupa na vláknech φ s operací definovanou pomocí reprezentantů: pokud X je vlákno nad a a Y je vlákno nad b , pak prvek $XY \in G/K$ je vlákno nad ab .

POZNÁMKA 3.5. To, že faktor grupa má skutečně vlastnosti grupy, se lehce ověří z platnosti těchto vlastností v G .

3.1 Levé a pravé třídy

Věta 3.6. Mějme homomorfismus $\varphi : G \rightarrow H$ s jádrem $\text{Ker } \varphi = K$ a necht' $X_a \in G/K$ je vlákno nad $a \in H$, tedy $X_a = \varphi^{-1}(a)$. Potom platí:

1. $\forall u \in X_a$ je $X_a = \{uk | k \in K\}$,
2. $\forall u \in X_a$ je $X_a = \{ku | k \in K\}$.

Důkaz. Dokážeme pouze první bod (druhý se dokazuje analogicky). Označme $uK = \{uk | k \in K\}$, mějme $u \in X_a$ (tedy $\varphi(u) = a$) a ukážeme, že $uK \subset X_a$: $\varphi(uk) = \varphi(u)\varphi(k) = \varphi(u)e = a$. (Využili jsme nejprve toho, že φ je homomorfismus a pak toho, že k je z jádra.) Pro důkaz opačné inkluze mějme libovolné $g \in X_a$ a vezměme $k = u^{-1}g$. Jelikož $\varphi(k) = \varphi(u^{-1}g) = \varphi(u^{-1})\varphi(g) = a^{-1}a = e$, k patří do jádra. Dále zřejmě $g = uk$, tedy $g \in uK$. $\square$

POZNÁMKA 3.7. Právě dokázaná věta nás opravňuje považovat vlákna a množiny $uK = Ku$ za třídy ekvivalence vzhledem k ekvivalenci $a \sim b \Leftrightarrow a = kb$ pro nějaké $k \in K$. (Triviální ověření vlastností ekvivalence je přenecháno čtenáři.)

Definice 3.8. Pro libovolnou $H \leq G$ a libovolné $g \in G$ nazýváme množiny $gH = \{gh | h \in H\}$ respektive $Hg = \{hg | h \in H\}$ **levé** respektive **pravé třídy** H v G . Libovolný prvek třídy nazýváme jejím **reprezentantem**.

Věta 3.9. Buďte G grupa a K jádro nějakého homomorfismu φ z G do nějaké grupy. Potom množina levých tříd K v G s operací definovanou jako $aK \otimes bK = (ab)K$ je grupa G/K . Tedy tato operace je dobře definovaná (nezávisí na výběru reprezentanta). (Obr. 3.2)

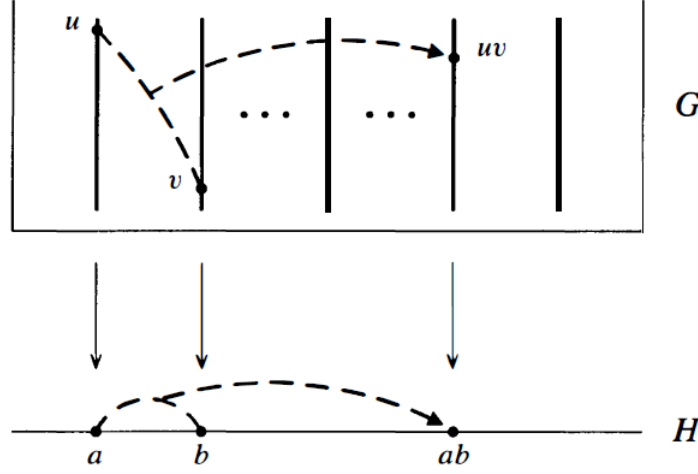
Důkaz. Mějme $X, Y \in G/K$, $X = \varphi^{-1}(a)$, $Y = \varphi^{-1}(b)$ a $Z = XY \in G/K$. Podle definice operací v G/K je $Z = \varphi^{-1}(ab)$. Z věty 3.6 víme, že prvky G/K jsou levé třídy K . Je třeba ukázat, že i operace, kterou zde definuje pomocí reprezentantů odpovídá původní definici násobení v G/K bez ohledu na výběr reprezentanta. Mějme $u \in X$ a $v \in Y$, tedy $\varphi(u) = a$, $\varphi(v) = b$ a $X = uK$ a $Y = vK$. Určíme, zda $uv \in Z$.

$$\varphi(uv) = \varphi(u)\varphi(v) = ab$$

Odtud tedy plyne, že $uv \in Z$, a tedy $Z = uvK$. $\square$

Věta 3.10. Necht' $N \leq G$, potom množina levých tříd N v G tvoří rozklad G (jejich sjednocením je G a jednotlivé třídy mají prázdný průnik). Dále $\forall u, v \in G$ platí $uN = vN$ právě tehdy, když $u^{-1}v \in N$, tedy když u a v jsou reprezentanty stejné třídy.

3 Faktor grupy



Obrázek 3.2: Znázornění násobení v G/K pomocí reprezentantů levých tříd. Převzato z [1].

Důkaz. Nejprve ukážeme, že sjednocením levých tříd je celé G . Jelikož N je grupa, pak $e \in N$, a tedy platí:

$$\bigcup_{g \in G} gN \supset \bigcup_{g \in G} ge = G.$$

Pro důkaz druhé části vezmeme $uN \cap vN \neq \emptyset$ a ukážeme, že potom platí $uN = vN$. Vezmeme $x \in uN \cap vN$, tedy x můžeme napsat jako $x = un_1 = vn_2$ pro nějaká $n_1, n_2 \in N$. Rovnost vynásobíme zprava n_1^{-1} a dostaneme $u = vn_2n_1^{-1} = vn_3$ pro nějaké $n_3 \in N$. Tedy vidíme, že $u \in vN$. Dále pro libovolné $t \in uN$ platí $t = un_4 = (vn_3)n_4 = vn_5$, takže $t \in vN$ pro $\forall t \in uN$, tedy $uN \subset vN$. Opačnou inkluzi dostaneme záměnou role u a v .

Jelikož víme, že $u = vn_3$, pak platí $v^{-1}u = n_3$, tedy $v^{-1}u \in N$ a to platí pro libovolné reprezentanty tříd. $\square$

POZNÁMKA 3.11. Právě dokázaná věta říká, že levé třídy jsou třídy ekvivalence vzhledem k ekvivalenci $a \sim b \Leftrightarrow a = nb$ pro nějaké $n \in N$ a G je tedy rozloženo do tříd ekvivalence.

Věta 3.12. *Bud' G grupa a $N \leq G$. Potom:*

1. *Operace na levých třídách definovaná jako $uNvN = (uv)N$ je dobře definovaná právě tehdy, když $(gng^{-1} \in N)(\forall g \in G \text{ a } \forall n \in N)$.*
2. *Je-li výše uvedená operace dobře definovaná, pak je množina levých tříd N grupou s jednotkou eN a inverzním prvkem $(gN)^{-1} = g^{-1}N$.*

Důkaz. 1. $\Rightarrow$) Nechť je operace na levých třídách dobře definovaná, tedy

$$(\forall u, v \in G)(u, u_1 \in uN \text{ a } v, v_1 \in vN \Rightarrow uvN = u_1v_1N). \quad (3.1)$$

Nechť $g \in G$ a $n \in N$ libovolné. Položíme $u = e$, $u_1 = n$ a $v = v_1 = g^{-1}$ a z předpokladu dostaneme

$$g^{-1}N = ng^{-1}N \quad (3.2)$$

3 Faktor grupy

Protože $e \in N$, $ng^{-1} \in g^{-1}N$. Tedy $ng^{-1} = g^{-1}n_1$, pro nějaké $n_1 \in N$. Vynásobením g zleva dostáváme požadovanou rovnost $gng^{-1} = n_1 \in N$.

$\Leftrightarrow$) Předpokládáme $(gng^{-1} \in N)(\forall g \in G \text{ a } \forall n \in N)$ a vezmeme $u, u_1 \in uN$ a $v, v_1 \in vN$. Pak můžeme psát $u_1 = un$ a $v_1 = vm$ pro nějaké $n, m \in N$. Musíme ukázat, že $u_1v_1 \in uvN$:

$$u_1v_1 = (un)(vm) = u(vv^{-1})nvm = (uv)(v^{-1}nv)m = (uv)(n_1)m = uvn_2 \in uvN, \quad (3.3)$$

kde $n_1 = v^{-1}nv = (v^{-1})n(v^{-1})^{-1} \in N$ z předpokladu a $n_2 = n_1m \in N$ z definice. Protože $u_1v_1 \in uvN \cap u_1v_1N$, plyne z předchozí věty rovnost $uvN = u_1v_1N$.

2. Je-li operace na levých třídách dobře definovaná, axiomy grupy se přenášejí z G . Asociativita:

$$(uN)(vNwN) = uN(vwN) = u(vw)N = (uv)wN = (uNvN)(wN), \quad \forall u, v, w \in G \quad (3.4)$$

Z definice násobení je vidět že jednotka v G/N je N a $g^{-1}N$ je inverze gN . □

3.2 Normální podgrupy

Definice 3.13. Prvek $m = gng^{-1}$ se nazývá **konjugovaný** k n prvkem g .

Definice 3.14. Buď $A \subset G$ libovolná podmnožina grupy. Množina $M = gAg^{-1}$ se nazývá **konjugovaná** k A prvkem g .

Definice 3.15. Pokud pro $N \leq G$ platí $N_G(N) = G$ (normalizátor N v G), pak N nazýváme **normální** podgrupa. Značíme $N \trianglelefteq G$

POZNÁMKA 3.16. Pro ověření, zda podgrupa $N \leq G$ je normální, stačí ověřit, že komutuje s generátory množiny $G \setminus N$ (množinový rozdíl), pokud tyto generátory známe.

Věta 3.17. *Nechť $N \leq G$, potom následující tvrzení jsou ekvivalentní:*

1. $N \trianglelefteq G$
2. $N_G(N) = G$
3. $gN = Ng$ pro $\forall g \in G$.
4. Operace na třídách je dobře definovaná.
5. $gNg^{-1} \subset N$ pro $\forall g \in G$.

Důkaz. Přepsání definic a věta 3.12. □

Věta 3.18. *Nechť $N \leq G$, potom $N \trianglelefteq G$ právě tehdy když $\exists$ homomorfismus φ takový, že $N = \text{Ker } \varphi$.*

Důkaz. $\Leftrightarrow$) Podle věty 3.6 víme, že levé a pravé třídy jsou stejné ($gN = Ng$), což je podle věty 3.17 ekvivalentní normálnosti grupy.

3 Faktor grupy

$\Rightarrow$) Nyní máme $N \trianglelefteq G$ a označíme $H = G/N$ (podle věty 3.17 je operace na levých třídách pro normální grupu dobře definovaná). Definujeme zobrazení $\pi : G \rightarrow G/N$ jako $\pi(g) = gN$ pro $\forall g \in G$. Z definice operací v G/N platí pro $\forall f, g \in G$: $\pi(fg) = (fg)N = fNgN = \pi(f)\pi(g)$, tedy π je homomorfismus. Jeho jádro je: $\text{Ker}(\pi) = \{g \in G \mid \pi(g) = eN\} = \{g \in G \mid gN = eN\} = \{g \in G \mid g \in N\} = N$.

□

POZNÁMKA 3.19. Nyní můžeme faktorizovat podle normální podgrupy G/N , aniž bychom měli homomorfismus.

Definice 3.20. Buď $N \trianglelefteq G$, pak zobrazení $\pi : G \rightarrow G/N : \pi(g) = gN$ nazýváme **přirozená projekce** G na G/N .

3.3 Index grupy, Lagrangeova věta

Věta 3.21 (Lagrange). *Nechť G je konečná, $H \leq G$, potom $|H|$ dělí $|G|$. Navíc počet levých tříd H v G je roven $\frac{|G|}{|H|}$.*

Důkaz. Nejprve ukážeme, že všechny levé třídy mají stejně prvků. Definujme zobrazení $f : aH \rightarrow bH$ mezi libovolnými dvěma levými třídami aH a bH předpisem $f(x) = ba^{-1}x$. Protože zobrazení s předpisem $f^{-1}(y) = ab^{-1}y$ je zřejmě inverzní k f , je f bijekce mezi levými třídami, a ty tedy mají stejný počet prvků.

Označme $|H| = |eH| = n$ a k počet levých tříd. G rozděleno na k levých tříd o n prvcích, platí $|G| = kn$, a tedy $k = \frac{|G|}{n}$. □

POZNÁMKA 3.22. První část důkazu (všechny levé třídy mají stejně prvků) platí i pro nekonečné grupy.

POZNÁMKA 3.23. Komutativní grupa prvočíselného řádu nemůže mít netriviální normální podgrupu.

Definice 3.24. Buď G grupa (i nekonečného řádu) a $H \leq G$. Potom počet levých tříd H v G nazýváme **index** H v G a značíme $|G : H|$.

POZNÁMKA 3.25. Nechť $H \leq G$ má index $|G : H| = 2$. Potom je H normální podgrupou, protože rozklady do levých a pravých tříd $G = H \cup gH = H \cup Hg$ implikuje rovnost $gH = Hg$.

POZNÁMKA 3.26. Pro konečné grupy tedy platí $|G : H| = \frac{|G|}{|H|}$.

Důsledek 3.27. Pro konečnou grupu G a $x \in G$ platí $|x|$ dělí $|G|$.

Důkaz. Díky nerovnosti $|x| < |G|$, dokázané v pozn. 1.29, a konečnosti $|G|$ tvoří mocniny x cyklickou podgrupu G . □

Důsledek 3.28. Grupa prvočíselného řádu je cyklická.

Věta 3.29 (Cauchy). *Nechť grupa G má řád $|G| = n \in \mathbb{N}$ a p je prvočíslo, které dělí n . Pak existuje prvek $x \in G$ s řádem $|x| = p$*

Důkaz. Protože máme konečnou grupu, řád prvku x dělí řád grupy G . Proto pro každé $x \in G$ a k řád x platí $x^n = (x^k)^{\frac{n}{k}} = e$. Protože p dělí n , tj. $n = pk$, platí $x^n = x^{kp} = (x^k)^p = e$, tj. x^k má řád p . □

3 Faktor grupy

Definice 3.30. Grupu G , jejíž jediné normální podgrupy jsou triviální (e a G), nazýváme **prostá**.

POZNÁMKA 3.31. Opačné tvrzení k Lagrangeově větě neplatí. Tedy konečná grupa G , jejíž řád má dělitele n , nemusí mít podgrupu řádu n . (Platí to pro konečné abelovské grupy.)

3.4 Součinnová podgrupa

Definice 3.32. Zavádíme „součin“ podgrup $K, H \leq G$ jako: $HK = \{kh | k \in K, h \in H\}$.

Věta 3.33. *Nechť H a K jsou podgrupy konečné grupy G , pak*

$$|HK| = \frac{|H||K|}{|H \cap K|}. \quad (3.5)$$

Důkaz. HK můžeme napsat jako sjednocení levých tříd K ,

$$HK = \bigcup_{h \in H} hK. \quad (3.6)$$

Protože všechny levé třídy mají stejný počet prvků $|K|$, stačí zjistit počet různých levých tříd tvaru $hK, h \in H$. Ale $h_1K = h_2K$ pro $h_1, h_2 \in H$, právě když $h_2^{-1}h_1 \in K$. Tedy

$$h_1K = h_2K \Leftrightarrow h_2^{-1}h_1 \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K). \quad (3.7)$$

To znamená, že počet různých levých tříd tvaru $hK, h \in H$ je stejný jako počet levých tříd tvaru $h(H \cap K), h \in H$. A to je, z Lagrangeovy věty, rovno $\frac{|H|}{|H \cap K|}$. Tedy HK obsahuje $\frac{|H|}{|H \cap K|}$ různých levých tříd K , kde každá má $|K|$ prvků, čímž dostáváme tvrzení věty. $\square$

Věta 3.34. *Nechť $H, K \leq G$, pak $HK \leq G$ právě tehdy, když $HK = KH$.*

Důkaz. $\Leftarrow$) Nechť $HK = KH$ a $a, b \in HK$. Ukážeme, že $ab^{-1} \in HK$, takže HK je podgrupa. Můžeme psát $a = h_1k_1$ a $b = h_2k_2$ pro nějaké $h_1, h_2 \in H$ a $k_1, k_2 \in K$. Tedy

$$ab^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1k_3h_2^{-1} \quad (3.8)$$

kde $k_3 = k_1k_2^{-1} \in K$. Užitím předpokladu můžeme napsat $k_3h_2^{-1} = h_4k_4$ a dostáváme

$$ab^{-1} = (h_1h_4)k_4 \in HK. \quad (3.9)$$

$\Rightarrow$) Vezměme $a \in KH$. Pak $a = kh$ a platí $a^{-1} = (kh)^{-1} = h^{-1}k^{-1} \in HK$. Protože HK je podgrupa, je i $a \in HK$ a tudíž $KH \subset HK$. Pro důkaz opačné inkluze vezmeme $hk \in HK$. Protože HK je podgrupa, můžeme psát $hk = a^{-1}$ pro nějaké $a \in HK$. Ale taky $a = h_1k_1$ pro nějaké $h_1 \in H, k_1 \in K$. Dostáváme tedy

$$hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH. \quad (3.10)$$

$\square$

Důsledek 3.35. *Nechť $H, K \leq G$ a $H \leq N_G(K)$, pak $HK \leq G$. Speciálně pokud $K \trianglelefteq G$, pak $HK \leq G$ pro libovolnou $H \leq G$.*

3 Faktor grupy

Důkaz. Ukážeme že $HK = KH$. Necht' $h \in H$, $k \in K$. Z předpokladu máme $hkh^{-1} \in K$, tudíž

$$hk = (hkh^{-1})h \in KH. \quad (3.11)$$

Ukázali jsme tedy, že $HK \subset KH$. Opačná inkluze se ukáže analogicky a z předchozí věty už plyne, co jsme chtěli dokázat. $\square$

3.5 Věty o isomorfismech

Věta 3.36 (1. VOI). *Pokud $\varphi : G \rightarrow H$ je homomorfismus, pak $\text{Ker } \varphi \trianglelefteq G$ a $G/\text{Ker } \varphi \cong \varphi(G)$.*

Důkaz. První část je zřejmá z vět 3.6 a 3.17. Důkaz druhé spočívá v ověření, že $\varphi' : G/\text{Ker } \varphi \rightarrow \varphi(G) : \varphi'(g\text{Ker } \varphi) = \varphi(g)$ je izomorfismus, což je ponecháno jako cvičení. $\square$

Důsledek 3.37. *Bud' $\varphi : G \rightarrow H$ homomorfismus. Potom platí:*

1. φ je monomorfni, právě když $\text{Ker } \varphi = e$,
2. $|G : \text{Ker } \varphi| = |\varphi(G)|$.

Věta 3.38 (2. VOI, „diamantová“). *Bud' G grupa a $A \leq G$, $B \leq G$ a $A \leq N_G(B)$. Potom $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ a $AB/B \cong A/A \cap B$.*

Důkaz. Z důsledku 3.35 plyne, že $AB \leq G$. Protože $A \leq N_G(B)$ z předpokladu a $B \leq N_G(B)$ triviálně, je taky $AB \leq N_G(B)$, tedy $B \trianglelefteq AB$ a faktorgrupa AB/B je dobře definována. Definujeme proto homomorfismus $\varphi : A \rightarrow AB/B$ předpisem $\varphi(a) = aB$:

$$\varphi(a_1a_2) = (a_1a_2)B = a_1Ba_2B = \varphi(a_1)\varphi(a_2). \quad (3.12)$$

Z definice je vidět, že φ je surjektivní. Jednotkový prvek v AB/B je B , tedy $\text{Ker } \varphi = \{a \in A, aB = B\} = A \cap B$. Z 1. VOI už plyne, že $A \cap B \trianglelefteq A$ a $A/A \cap B \cong AB/B$. $\square$

Věta 3.39 (3. VOI). *Bud' G grupa a $H \trianglelefteq G$, $K \trianglelefteq G$ a $H \leq K$. Potom $K/H \trianglelefteq G/H$ a $(G/H)/(K/H) \cong G/K$. Označíme-li faktorgrupu podle H pruhem, tvrzení lze přepsat ve tvaru $\bar{G}/\bar{K} \cong G/K$.*

Důkaz. H komutuje se všemi prvky G , tím spíše s prvky z K , takže $K \trianglelefteq H$ a K/H má smysl. Příným výpočtem za využití normality podgrup ověříme platnost $K/H \trianglelefteq G/H$:

$$\begin{aligned} gHkH(gH)^{-1} &= gH(g^{-1}g)k(g^{-1}g)Hg^{-1}H = (gHg^{-1})(gkg^{-1})(gHg^{-1})H = \\ &= Hk_1H = (k_1k_1^{-1})Hk_1H = k_1H \in K/H. \end{aligned} \quad (3.13)$$

Definujeme homomorfismus $\varphi : G/H \rightarrow G/K$ předpisem $\varphi(gH) = gK$. Abychom ukázali že φ je dobře definované, vezmeme $g_1H = g_2H$. Potom $g_1 = g_2h$ pro nějaké $h \in H$. Protože $H \leq K$, je taky $h \in K$, proto $g_1K = g_2K$. Tudíž $\varphi(g_1H) = \varphi(g_2H)$ a φ je dobře definované. Protože g může být libovolné, je φ taky surjektivní. Dále

$$\text{Ker } \varphi = \{gH \in G/H \mid \varphi(gH) = K\} = \{gH \in G/H \mid gK = K\} = \{gH \in G/H \mid g \in K\} = K/H, \quad (3.14)$$

z 1. VOI už plyne $(G/H)/(K/H) \cong G/K$. $\square$

3 Faktor grupy

POZNÁMKA 3.40. Následující věta hovoří o vztahu struktury podgrup původní grupy G a faktorgrupy G/N . Vlastně říká, že struktura podgrup faktorgrupy je stejná jako struktura podgrup G , které obsahují N .

Věta 3.41. [4. VOI, „mřížková“] *Bud' G grupa a $N \trianglelefteq G$. Potom existuje bijekce θ z množiny podgrup G obsahujících N na množinu podgrup G/N , která každé podgrupě A z první množiny přiřazuje podgrupu A/N ze druhé. Zobrazení θ má navíc tyto vlastnosti: Pro $A, B \leq G$ obsahující N jako podgrupu platí*

1. $B \leq A \Leftrightarrow B/N \leq A/N$,
2. Je-li $A \leq B$, pak $|B : A| = |B/N : A/N|$,
3. $\langle A, B \rangle / N = \langle A/N, B/N \rangle$,
4. $A/N \cap B/N = (A \cap B)/N$,
5. $A \trianglelefteq G \Leftrightarrow A/N \trianglelefteq G/N$.

Důkaz. Ověříme, že zobrazení θ definované pomocí $A \mapsto A/N$ je bijekce: Nejprve prostota. Nechť $A/N = B/N$. Pak $\forall a \in A$ platí $aN = bN$ pro nějaké $b \in B$, tj. $a^{-1}b \in N \subset B$. Proto $a \in B$ a $A \subset B$. Druhá inkluze se dokáže stejně.

Nyní surjektivita: Je-li S podgrupa G/N , a $\phi : G \rightarrow G/N$, pak $\phi^{-1}(S) = \{s \in G | sN \in S\}$ je podgrupa G (platí $uNvN = uvN$) obsahující $N = \phi^{-1}(\{e\})$ a $\theta(\phi^{-1}(S)) = \{sN | sN \in S\} = S$, což dokazuje surjektivitu.

Nyní ověříme vlastnosti:

1. Z $A \leq B$ plyne $A/N \leq B/N$ díky tomu, že operace na levých třídách je díky $N \trianglelefteq G$ dobře definovaná, obráceně proto, že θ je bijekce.
2. Zobrazení ψ zobrazuje levé třídy v B/A do levých tříd v $(B/N)/(A/N)$ tak, že pro $b \in B$ zobrazí bA na $(bN)(A/N)$. ψ je dobře definované a prosté, protože $b_1A = b_2A \Leftrightarrow b_1^{-1}b_2 \in A \Leftrightarrow (b_1N)^{-1}(b_2N) \in (A/N) \Leftrightarrow (b_1N)(A/N) = (b_2N)(A/N)$. ψ je také surjektivní, protože v $(bN)(A/N)$ prochází b celé B , a tedy ψ je izomorfismus.
3. Protože $N \trianglelefteq G$, je operace na levých třídách dobře definovaná. Proto pro důkaz inkluze $\langle A, B \rangle / N \subset \langle A/N, B/N \rangle$ stačí ověřit $xN \subset \langle A/N, B/N \rangle$ pro $x \in A$ nebo $x \in B$. To ale zřejmě platí, protože $x \in A$ implikuje $xN \in A/N$, stejně pro $x \in B$. Podobně pro inkluzi $\langle A/N, B/N \rangle \subset \langle A, B \rangle / N$ stačí ověřit, že $xN \in A/N$ nebo $xN \in B/N$ implikuje $x \in \langle A, B \rangle$. Nechť tedy $xN \in A/N$, pak $xN = aN$ pro nějaké $a \in A$, tudíž $a^{-1}x \in N \subset A \subset \langle A, B \rangle$ a stejně pro $xN \in B/N$.
4. Stejně jako bod 3.
5. Předpokládejme nejprve $A \trianglelefteq G$. Pak pro $aN \in A/N$ platí $gNaNg^{-1}N = gag^{-1}N = a_1N \in A/N$, tedy $A/N \trianglelefteq G/N$.

Obrácená implikace: Nechť $A/N \trianglelefteq G/N$. Definujme zobrazení $\sigma : G \rightarrow (G/N)/(A/N) : g \mapsto (gN)(A/N)$. Toto zobrazení vzniklo jako složení homomorfismů (přirozených projekcí) z G do G/N a z G/N do $(G/N)/(A/N)$, je to tedy homeomorfismus. Platí, že $\text{Ker } \sigma = A$, protože $g \in \text{Ker } \sigma \Leftrightarrow (gN)(A/N) = (A/N) \Leftrightarrow gN \in A/N$, tedy $gN = aN$ pro nějaké $a \in A$. Protože platí $N \leq A$, je to ekvivalentní $g \in A$, A je jádrem homomorfismu, a tudíž normální podgrupou G .

□

3.6 Kompoziční řady

Věta 3.42. *Je-li G konečná Abelovská grupa a p prvočíslo, které dělí $|G|$, pak G obsahuje prvek řádu p .*

Důkaz. Důkaz se provádí pomocí takzvané úplné indukce podle řádu G . Tedy se předpokládá, že tvrzení platí pro všechny grupy řádu ostře menšího než $|G|$ a ukáže se platnost pro $|G|$. Pro $|G| = 1$ je tvrzení triviální.

Mějme $|G| > 1$, tedy existuje $x \in G, x \neq e$. Pokud $|G| = p$ je v důsledku Lagrangeovy věty 3.21 G cyklická a tedy generovaná nějakým prvkem řádu $|G|$. Dále tedy předpokládejme $|G| > p$.

Pokud bychom vzali prvek, jehož řád je dělitelný číslem p (tedy $|x| = pn$), pak stačí vzít prvek x^n , který je řádu $|x^n| = p$. Dále tedy uvažujeme $p \nmid |x|$.

Bud' $N = \langle x \rangle$. Jelikož G je abelovská, pak $N \trianglelefteq G$ a z Lagrangeovy věty máme $|G/N| = \frac{|G|}{|N|}$, respektive $|G/N||N| = |G|$. Protože $|N| > 1$, musí platit $|G/N| < |G|$. Dále jelikož $p \mid |G|$, ale $p \nmid |N|$, musí platit $p \mid |G/N|$. Z indukčního předpokladu pak G/N obsahuje prvek $\bar{y} = yN$ řádu p . Označme řád prvku y v G roven m . Pak jistě $(yN)^m = y^m N = eN$ proto $p \mid |y|$ a dostáváme se k předchozímu případu. $\square$

Definice 3.43. Grupa G (konečná i nekonečná) se nazývá **jednoduchá**, pokud $|G| > 1$ a jejími jedinými normálními podgrupami jsou e a G .

Definice 3.44. V grupě G řádu podgrup (řetěz) $e = N_0 \leq N_1 \leq \dots \leq N_{k-1} \leq N_k = G$ nazýváme **kompoziční řada**, pokud $(\forall i, 0 \leq i \leq k-1)(N_i \trianglelefteq N_{i+1})$ a N_{i+1}/N_i je jednoduchá. Faktor grupy N_{i+1}/N_i se pak nazývají **kompoziční faktory** G .

Věta 3.45 (Jordan-Hölder). *Bud' $G \neq e$ konečná grupa. Pak:*

1. G má kompoziční řadu,
2. kompoziční faktory této řady jsou dány jednoznačně. Konkrétně pokud $e = N_0 \leq N_1 \leq \dots \leq N_r = G$ a $e = M_0 \leq M_1 \leq \dots \leq M_s = G$ jsou dvě kompoziční řady G , pak $r = s$ a existuje permutace π r -tice $(1, 2, \dots, r)$ taková, že

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1} \quad 1 \leq i \leq r. \quad (3.15)$$

Důkaz J-H první část. Mějme nejdelší možný řetěz normálních podgrup podgrup

$$e = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_r = G.$$

Sporem dokážeme, že N_{i+1}/N_i je jednoduchá pro všechna i : Kdyby existovalo i tak, že N_{i+1}/N_i není jednoduchá, pak existuje $H \trianglelefteq N_{i+1}/N_i$, $H \neq \{e\}$, $H \neq N_{i+1}/N_i$. Vezmu-li $\pi^{-1}(H)$, tj. vzor H při projekci $\pi : N_{i+1} \rightarrow N_{i+1}/N_i$, pak ze 4.VOI 3.41 plyne $\pi^{-1}(H) \trianglelefteq N_{i+1}$ a N_i je jádro projekce $\tilde{\pi} : \pi^{-1}(H) \rightarrow N_i$, tj. $N_i \trianglelefteq \pi^{-1}(H)$, takže by bylo možné $\pi^{-1}(H)$ „vřadit“ do řetězu a vytvořili bychom delší řetěz, což je spor s předpokládanou maximalitou. $\square$

Pro důkaz druhé části nejprve vyslovíme a dokážeme následující lemma:

Lemma 3.46. *Nechť G je grupa, M, N její normální podgrupy, $M \neq N$, G/M a G/N jednoduché. Potom $G = NM$ a platí $M/(M \cap N) \cong G/N$ a $N/(M \cap N) \cong G/M$.*

3 Faktor grupy

Důkaz. M není podgrupa N (a obráceně), protože jinak by díky 4. VOI byla N/M normální podgrupou G/M různou od G/M a $\{e\}$ ($M \neq N$), což je spor s jednoduchostí.

Protože $M, N \trianglelefteq G$, pak i $NM \trianglelefteq G$ (všichni reprezentanti komutují se vším). Tudíž platí, že $NM/M \trianglelefteq G/M$. Protože je ale G/M jednoduchá, musí NM/M být buď G/M nebo $\{e\}$. Druhá varianta však nenastává, protože jinak by $MN = M$ a $N \leq M$. Tudíž $MN/M = G/M$ a $MN = G$. Potom závěry $M/(M \cap N) \cong G/N$ a $N/(M \cap N) \cong G/M$ plynou z 2. VOI 3.38. $\square$

Důkaz J–H druhá část. Důkaz provedeme úplnou indukcí v r : Pokud je $r = 1$, pak i $s = 1$, protože $\{e\} \trianglelefteq G$ je jediný přípustný řetěz.

Nyní indukční krok $r = 1, \dots, n - 1 \rightarrow n$: Mějme dva řetězy normálních podgrup

$$e = N_0 \leq N_1 \leq \dots \leq N_r = G, \quad e = M_0 \leq M_1 \leq \dots \leq M_s = G.$$

Pokud $N_{r-1} = M_{s-1}$, pak je věta splněna z indukčního předpokladu, takže nadále předpokládáme $N_{r-1} \neq M_{s-1}$. Pro zkrácení zápisu si označím $M_{s-1} = M$ a $N_{r-1} = N$ a definuji $K = M \cap N$. Díky indukčnímu předpokladu má K kompozitní řadu

$$e = K_0 \leq K_1 \leq \dots \leq K_t = K.$$

K je normální podgrupa M a N (2. VOI 3.38), proto rozšířením kompozitní řady pro K získáme kompozitní řady pro M a N , konkrétně

$$e = K_0 \leq K_1 \leq \dots \leq K_t = K \leq M, \quad e = K_0 \leq K_1 \leq \dots \leq K_t = K \leq N.$$

Díky indukčnímu předpokladu platí $r - 1 = t + 1 = s - 1$ (stejně délky řetězů), tj. $r = s$, a také vlastnost vůči permutacím faktorgrup. Díky dokázanému lemmatu pak platí také $N/(M \cap N) \cong G/M$, což je $N_{r-1}/(N_{r-1} \cap M_{s-1}) \cong M_s/M_{s-1}$, takže permutační vlastnost faktorgrup platí na celých kompozitních řadách

$$e = N_0 \leq N_1 \leq \dots \leq N_r = G, \quad e = M_0 \leq M_1 \leq \dots \leq M_s = G.$$

$\square$

Věta 3.47. *Existuje 18 (nekonečných) rodin jednoduchých grup a 26 jednoduchých grup, které nepatří do žádné z těchto skupin (sporadické jednoduché grupy) takových, že každá konečná jednoduchá grupa je isomorfní s některou z výše uvedených.*

Důkaz. Výsledek cca 100 let práce mnoha matematiků na 5000-10000 stránkách odborných časopisů. Ponecháno čtenáři jako snadné cvičení. $\square$

Věta 3.48 (Důsledek Feit–Thompsonovy věty). *Všechny jednoduché konečné grupy lichého řádu jsou abelovské, přesněji $|G| = 2n - 1 \Leftrightarrow 2n + 1 = p, G \cong \mathbb{Z}_p$.*

Důkaz. 255 stran... $\square$

4 Akce grupy na množině

Definice 4.1. Akcí grupy G na množině A nazveme zobrazení $\cdot : G \times A \rightarrow A$ (značíme $g \cdot a$), které splňuje:

1. $(\forall g_1, g_2 \in G)(\forall a \in A)(g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a)$,
2. $(\forall a \in A)(e \cdot a = a)$.

Věta 4.2. Bud' $\cdot$ akce grupy G na množině A . Zaved'me pro pevně zvolené $g \in G$ zobrazení $\sigma_g : A \rightarrow A$ vztahem $(\sigma_g(a) = g \cdot a)(\forall a \in A)$. Potom platí:

1. $(\forall g \in G)$ je zobrazení σ_g permutací množiny A ,
2. zobrazení $\varphi : G \rightarrow S_A$ (permutace množiny A) definované $\varphi(g) = \sigma_g$ je homomorfismus.

Důkaz. 1) Dokážeme, že σ_g má oboustrannou inverzi, a to konkrétně $(\sigma_g)^{-1} = \sigma_{g^{-1}}$. Z vlastností akce platí: $(\sigma_{g^{-1}} \circ \sigma_g)(a) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = e \cdot a = a$. Záměnou g za g^{-1} dostaneme, že také $(\sigma_g \circ \sigma_{g^{-1}})(a) = a$.

2) Z bodu 1) víme, že skutečně $\sigma_g \in S_A$. Nyní jen ukážeme, že $\forall a \in A$ a $\forall f, g \in G$ platí $(\varphi(f) \circ \varphi(g))(a) = \sigma_f(\sigma_g(a)) = f \cdot (g \cdot a) = (fg) \cdot a = \sigma_{fg}(a) = \varphi(fg)(a)$. □

Důsledek 4.3. Pro každou grupu G a neprázdnou množinu A existuje bijekce mezi akcemi G na množině A a homomorfismy G do symetrické grupy S_A .

Důsledek 4.4. Vezmu-li za množinu A grupu G , pak dostanu tvrzení, že každý řádek (či sloupec) tabulky násobení je bijekcí množiny prvků, tj. každý prvek se v něm objeví právě jednou.

4.1 Stabilizátory a orbity

Definice 4.5. Mějme grupu G a její akci $\cdot : G \times S \rightarrow S$ na množinu S a nechť $s \in S$ je pevně zvolený prvek. Potom **stabilizátor** s v G je: $G_s = \{g \in G | g \cdot s = s\}$. **Orbita** s v G je $O_s = \{g \cdot s | g \in G\}$, občas značeno též $G \cdot s$.

Věta 4.6. Platí $G_s \leq G$.

Důkaz. Víme, že $e \in G_s$ z axiomu akce ($e \cdot s = s$). S využitím akce pak máme pro libovolné $y \in G_s$: $s = e \cdot s = (y^{-1}y) \cdot s = [\text{axiom akce}] = y^{-1} \cdot (y \cdot s) = y^{-1} \cdot s$, tedy $y^{-1} \in G_s$. Konečně pro $x, y \in G_s$ platí: $(xy) \cdot s = x \cdot (y \cdot s) = x \cdot s = s$, tedy i součin xy patří do G_s . □

Definice 4.7. Definujeme **jádro** akce jako: $\text{Ker}(\cdot) = \{g \in G | g \cdot s = s \text{ pro } \forall s \in S\}$.

Tvrzení 4.8. Platí, že $\text{Ker}(\cdot) \leq G$, navíc je průnikem všech stabilizátorů, tedy

$$\text{Ker}(\cdot) = \bigcap_{a \in A} G_a. \quad (4.1)$$

4 Akce grupy na množině

Definice 4.9. Řekneme, že akce je **věrná**, pokud $\text{Ker}(\cdot) = e$, respektive **tranzitivní**, existuje-li právě jedna orbita.

Věta 4.10. *Bud' $H \leq G$, akce G působí na levých třídách $\{g_i H\}_i = A$ a π_H permutační reprezentace. Potom*

1. G působí tranzitivně na A ,
2. stabilizátor eH v A je roven H ,
3. jádro akce je největší normální podgrupa H , tj.

$$\text{Ker}(\pi_H) = \bigcap_{x \in G} xHx^{-1}.$$

Důkaz. $\text{Ker}(\pi_H) = \{g \in G \mid gxH = xH, \forall x \in G\} = \{g \in G \mid x^{-1}gxH = H\}$, kde $x^{-1}gx \in H$, tj. $g \in xHx^{-1}$. $\square$

Věta 4.11 (Cayley). *Každá grupa je izomorfní nějaké podgrupě grupy permutací.*

Důkaz. Pan profesor nevyžaduje. Pro každé $g \in G$ definujeme zobrazení $\varphi_g : G \rightarrow G : x \mapsto \varphi_g(x) = gx \in G$. Z definice je zřejmé, že $\varphi_g^{-1} = \varphi_{g^{-1}}$, jedná se tedy o bijekci a $\varphi \in S_G$. S pomocí tohoto zobrazení vytvoříme hledaný izomorfismus tak, že $\Phi : G \rightarrow S_G, \Phi(g) = \varphi_g$. Díky asociativitě grupy G dostaneme, že se jedná o homomorfismus, protože platí

$$\Phi(g_1 g_2)x = (g_1 g_2)x = g_1(\Phi(g_2)x) = \Phi(g_1)\Phi(g_2)x.$$

Protože Φ zřejmě na $\text{Im } \Phi$ zobrazuje surjektivně, stačí ověřit prostotu: Díky krácení v grupě ale máme

$$\Phi(g_1) = \Phi(g_2) \Leftrightarrow \varphi_{g_1} = \varphi_{g_2} \Leftrightarrow (\text{aplikace na } x) \ g_1 x = g_2 x \Leftrightarrow g_1 = g_2.$$

Máme tudíž $G \cong \text{Im } \Phi$, což je podle předešlého tvrzení podgrupa S_G . $\square$

Důsledek 4.12. *Bud' p nejmenší prvo dělitel $|G|$ (G konečná) a podgrupa $H \leq G$ taková, že $|G : H| = p$. Potom $H \trianglelefteq G$.*

Důkaz. Pro řád G platí $|G| = p^s m$, kde $p \nmid m$. Definujme akci grupy G na levých třídách H předpisem $x \cdot (gH) = xgH$. Tato akce indukuje homomorfismus G na S_p (viz věta 4.2) a nechť K je jeho jádro. Díky 1.VOI je G/K izomorfní podgrupě S_p , tudíž $|G/K|$ dělí $p!$ Protože ale zároveň musí dělit $|G|$ a p je nejmenší prvo dělitel, pak $|G/K| = p$. Díky 3.VOI platí $|G/K| \cdot |G/H| = |K/H|$, z čehož plyne $p = |G/K| = |G/H| \cdot |K/H| = p|K/H|$. Rovnost $|K/H| = 1$ však znamená $H = K$, což je normální podgrupa G . $\square$

POZNÁMKA 4.13. Bud' G grupa a $S = \mathcal{P}(G)$. Pak G působí na S konjugací, tedy přiřazuje $B \mapsto gBg^{-1}$ pro $\forall B \in S$ a $g \in G$.

POZNÁMKA 4.14. Normalizátor $N_G(A)$ je tedy stabilizátor konjugace A v G .

4.2 Rovnice tříd

Věta 4.15. *Nechť G je grupa, A neprázdná množina. Pak platí:*

1. *Relace na A definovaná přes akci G jako $a \sim b \Leftrightarrow a = g \cdot b$ pro $g \in G$ je ekvivalence.*
2. *$\forall a \in A$ je počet prvků ve třídě ekvivalence obsahující a roven $|G : G_a|$ (indexu stabilizátoru a).*

Důkaz. 1. Reflexivita je jasná, pro ověření symetrie nechť $a \sim b$. Pak $a = g \cdot b$, takže $g^{-1} \cdot a = g^{-1} \cdot g \cdot b = b$, tedy $b \sim a$. Nakonec pro důkaz tranzitivity mějme $a \sim b$ a $b \sim c$, tedy $a = g \cdot b$ a $b = h \cdot c$ pro nějaké $g, h \in G$. Dostáváme $a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c$, proto $a \sim c$.

2. Sestrojíme bijekci mezi levými třídami G_a v G a třídami ekvivalence a (orbitami a). Nechť tedy $O_a = \{g \cdot a | g \in G\}$. Pak zobrazení $g \cdot a \mapsto gG_a$ zobrazuje O_a do množiny levých tříd G_a v G a je očividně surjektivní. Protože $g \cdot a = h \cdot a \Leftrightarrow h^{-1}g \in G_a \Leftrightarrow gG_a = hG_a$ je taky prosté.

□

POZNÁMKA 4.16. Konjugace splňuje axiomy akce a platí $G_s = C_G(s) = N_G(s)$ pro akci G na S , $s \in S$.

POZNÁMKA 4.17. Dále budeme pod pojmem orbita rozumět příslušnou třídu ekvivalence konjugace.

Věta 4.18 (rovnice tříd). *Nechť G je konečná grupa a $g_1, g_2, \dots, g_r$ reprezentanti různých orbit neobsažených v $Z(G)$. Pak*

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|.$$

Důkaz. Orbita x obsahuje jenom jeden prvek právě tehdy, když $x \in Z(G)$, protože $gxg^{-1} = x$ pro $\forall g \in G$. Nechť $Z(G) = \{e, z_2, \dots, z_m\}$ a $\{O_1, O_2, \dots, O_r\}$ buď orbity neobsažené v centru a g_i reprezentant O_i pro $\forall i$. Potom všechny orbity (třídy ekvivalence) jsou:

$$\{e\}, \{z_2\}, \dots, \{z_m\}, O_1, O_2, \dots, O_r.$$

Protože třídy ekvivalence tvoří disjunktní rozklad G , máme díky předchozí větě

$$|G| = \sum_{i=1}^m 1 + \sum_{i=1}^r |O_i| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|.$$

□

Důsledek 4.19. *Nechť P je grupa řádu $|P| = p^\alpha$, kde p je prvočíslo a $\alpha \in \mathbb{N}$. Pak $Z(P) \neq \{e\}$.*

Důkaz. Z rovnice tříd $|P| = |Z(P)| + \sum_{i=1}^r |P : C_P(g_i)|$ plyne, že $|Z(P)|$ je dělitelné p , protože $|P|$ je dělitelné p z předpokladu a $|P : C_P(g_i)|$ je dělitelné p z předpokladu a Lagrangeovy věty. ($C_P(g_i)$ je podgrupa P , takže její řád je p^i , kde i je menší než α , protože $Z(P)$ není prázdné.) Řád $|Z(P)|$ je tedy alespoň p , tj. větší než 1. □

Důsledek 4.20. *Grupa P řádu $|P| = p^2$ pro p prvočíslo je abelovská.*

Důkaz. $Z(P) \triangleleft P$. Proto $|P/Z(P)|$ musí být z množiny $\{1, p, p^2\}$. Protože $Z(P)$ obsahuje více než jeden prvek, p^2 to být nemůže. Sporem ukážeme, že to nemůže být p : Necht' $|P/Z(P)| = p$, pak $P/Z(P)$ je cyklická, tj. $P/Z(P) = \langle xZ(P) \rangle$. Potom ale bude P abelovská, protože prvky z P mají tvar $p_1 = x^k z_1$, kde $z_1 \in Z(P)$, a platí $p_1 p_2 = x^k z_1 x^l z_2 = x^{k+l} z_1 z_2 = p_2 p_1$ z definice z_1 a z_2 . To je ale implikuje $P = Z(P)$, což je spor s předpokladem. Celkově tudíž $|P/Z(P)| = 1$ a $Z(P) = P$ je abelovská. $\square$

5 Sylowova věta

Definice 5.1. Bud' G grupa a p prvočíslo.

1. Grupu řádu p^α pro nějaké $\alpha \geq 1$ se nazývá **p-grupa**. Podgrupy G řádu p^α nazýváme **p-podgrupy** G .
2. Je-li G řádu $p^\alpha m$ a $p \nmid m$, pak podgrupu řádu p^α nazýváme **Sylowova p-podgrupa** G .
3. Množinu všech Sylowových p -podgrup značíme $Syl_p(G)$ a počet těchto podgrup $n_p(G)$ (nebo jen n_p , je-li grupa jasná z kontextu).

Lemma 5.2. *Nechť $P \in Syl_p(G)$ a Q libovolná p -podgrupa G , pak $N_G(P) \cap Q = P \cap Q$.*

Důkaz. Nechť $H = N_G(P) \cap Q$. Protože $P \leq N_G(P)$, je jasné že $P \cap Q \leq H$, musíme tedy ukázat opačnou inkluzi. Z definice je $H \leq Q$, stačí proto ukázat, že $H \leq P$. Protože $H \leq N_G(P)$, je PH podgrupa a platí

$$|PH| = \frac{|P||H|}{|P \cap H|}.$$

Všechny členy na pravé straně jsou mocniny p , proto PH je p -podgrupa a protože $P \leq PH$ je p -podgrupa maximálního řádu, musí platit $|PH| = |P| = p^\alpha$, tedy $PH = P$ a $H \leq P$. $\square$

Věta 5.3 (Sylow). *Bud' G grupa řádu $p^\alpha m$, kde p je prvočíslo a $p \nmid m$. Pak:*

1. *Existuje Sylowova p -podgrupa, tedy $Syl_p(G) \neq \emptyset$.*
2. *Je-li P Sylowova p -podgrupa G a Q libovolná p -podgrupa G , pak existuje $g \in G$ takové, že $Q \leq gPg^{-1}$, tedy Q je obsažena v nějakém sdružení P . Speciálně každé dvě Sylowovy p -podgrupy G jsou vzájemně sdružené v G .*
3. *Počet Sylowových p -podgrup je tvaru $1 + kp$, tedy $n_p \equiv 1 \pmod{p}$. Dále n_p je index grupy $N_G(P)$ v G pro každou Sylowovu p -podgrupu P , a tedy $n_p | m$.*

Důkaz. 1. Důkaz provedeme úplnou indukcí na $|G|$, přičemž pro $|G| = 1$ není co dokazovat. Nechť tedy existuje Sylowova p -podgrupa pro všechny grupy menšího řádu než $|G|$.

Když $p \mid |Z(G)|$, pak podle věty 3.42 existuje $N \leq Z(G)$ řádu p . Pak $|\overline{G}| = |G/N| = p^{\alpha-1}m$ a z indukčního předpokladu existuje $\overline{P} \leq \overline{G}$ řádu $p^{\alpha-1}$. Takže pro P podgrupu G obsahující N takovou, že $P/N = \overline{P}$, platí $|P| = |P/N||N| = p^\alpha$ a P je Sylowova p -podgrupa G . Omezíme se proto na případ $p \nmid |Z(G)|$.

Nechť $g_1, g_2, \dots, g_r$ jsou reprezentanti různých tříd neobsažených v centru G , pak platí rovnice tříd

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|. \quad (5.1)$$

5 Sylowova věta

Pokud by platilo $p \mid |G : C_G(g_i)|, \forall i$, pak by platilo taky $p \mid |Z(G)|$, protože $p \mid |G|$. Proto pro nějaké i musí platit $p \nmid |G : C_G(g_i)|$. Označíme $H = C_G(g_i)$ pro dané i a máme

$$|H| = p^\alpha k, \quad \text{kde } p \nmid k, \quad m \times k \quad (5.2)$$

a jelikož $g_i \notin Z(G)$, $|H| < |G|$. Z indukčního předpokladu má H Sylowovu p -podgrupou P , která je taky podgrupou G . Navíc $|P| = p^\alpha$, takže P je Sylowova p -podgrupa G .

2. Nechť Q je libovolná p -podgrupa G a nechť

$$\mathcal{S} = \{gPg^{-1} \mid g \in G\} \stackrel{\text{ozn.}}{=} \{P_1, P_2, \dots, P_r\} = \mathcal{S}. \quad (5.3)$$

Z definice $\mathcal{S}$ může G , tedy taky Q , působit na $\mathcal{S}$ konjugací. $\mathcal{S}$ lze proto zapsat jako sjednocení orbit akce Q :

$$\mathcal{S} = O_1 \cup O_2 \cup \dots \cup O_s \quad (5.4)$$

kde $r = |O_1| + |O_2| + \dots + |O_s|$. Je potřeba si uvědomit, že r nezávisí na Q , ale počet orbit s ano (G má z definice jenom jednu orbitu na $\mathcal{S}$, ale Q jich může mít víc). Přeuspořádáme prvky $\mathcal{S}$ tak, aby prvních s bylo reprezentanty Q -orbit: $P_i \in O_i, 1 \leq i \leq s$. Pak z věty 4.15 plyne $|O_i| = |Q : N_Q(P_i)|$. Z definice platí $N_Q(P_i) = N_G(P_i) \cap Q$ a podle předchozího lemmatu, $N_G(P_i) \cap Q = P_i \cap Q$. Celkem tedy máme

$$|O_i| = |Q : P_i \cap Q|, \quad 1 \leq i \leq s. \quad (5.5)$$

Tedy můžeme ukázat, že $r \equiv 1 \pmod p$. Díky libovolnosti Q můžeme položit $Q = P_1$, takže

$$|O_1| = 1, \quad (5.6)$$

a $\forall i > 1, P_1 \neq P_i$, tedy $P_1 \cap P_i < P_1$, proto

$$|O_i| = |P_1 : P_1 \cap P_i| > 1, \quad 2 \leq i \leq s. \quad (5.7)$$

Protože P_1 je p -grupa, $|P_1 : P_1 \cap P_i|$ musí být mocnina p , tedy

$$p \mid |O_i|, \quad 2 \leq i \leq s. \quad (5.8)$$

Odtud

$$r = |O_1| + (|O_2| + \dots + |O_s|) \equiv 1 \pmod p \quad (5.9)$$

Nyní buď Q libovolná p -podgrupa G . Kdyby $Q \not\subseteq P_i, \forall i \in \hat{r}$, pak $Q \cap P_i < Q, \forall i$, tedy

$$|O_i| = |Q : Q \cap P_i| > 1, \quad 1 \leq i \leq s. \quad (5.10)$$

Tudíž $p \mid |O_i|, \forall i$ a $p \mid r$, což je spor s $r \equiv 1 \pmod p$. Proto $Q \leq gPg^{-1}$, pro nějaké $g \in G$.

Pro důkaz ekvivalence Sylowových p -podgrup stačí za Q volit libovolnou Sylowovu p -podgrupou. Pak $Q \leq gPg^{-1}$ a zároveň $|gPg^{-1}| = |Q| = p^\alpha$, proto $gPg^{-1} = Q$.

5 Sylowova věta

3. Stačí si uvědomit že $\mathcal{S} = \text{Syl}_p(G)$ protože každá Sylowova p -podgrupa je konjugovaná k P , tedy $n_p = r \equiv 1 \pmod{p}$. Nakonec díky 4.15 a tomu, že všechny Sylowovy p -podgrupy jsou konjugované, dostáváme

$$n_p = |G : N_G(P)|, \quad \forall P \in \text{Syl}_p(G). \quad (5.11)$$

□

Důsledek 5.4. *Bud' P Sylowova p -podgrupa grupy G . Potom následující tvrzení jsou ekvivalentní:*

1. P je jediná Sylowova p -podgrupa v G , tedy $n_p = 1$,
2. $P \trianglelefteq G$.

Důkaz. 1) $\Leftrightarrow$ 2): $n_p = 1$, znamená že pro všechna $g \in G$ platí $|gPg^{-1}| = |P|$, tudíž $gPg^{-1} = P$, tj. $P \trianglelefteq G$.

2) $\Leftrightarrow$ 1): $\forall g \in G, gPg^{-1} = P$. Necht' $\tilde{P} \in \text{Syl}_p(G)$. Pak $\tilde{P} = gPg^{-1} = P$. □

6 Přímý a polopřímý součin grup

Jedná se o způsob konstrukce větších grup z menších.

Definice 6.1. Přímý součin definujeme pro konečné a spočetně nekonečné množiny grup (rozdíl definice je jen formální).

1. **Přímým součinem** grup $G_1 \times G_2 \times \dots \times G_n$ s násobením $*_1, *_2, \dots, *_n$ po řadě, je množina n -tic $(g_1, g_2, \dots, g_n)$ ($g_i \in G_i$) s násobením definovaným po složkách. Tedy:

$$(g_1, g_2, \dots, g_n) * (h_1, h_2, \dots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_n *_n h_n). \quad (6.1)$$

2. **Přímým součinem** grup $G_1 \times G_2 \times \dots$ s násobením $*_1, *_2, \dots$, po řadě, je množina posloupností $(g_1, g_2, \dots)$ ($g_i \in G_i$) s násobením definovaným po složkách. Tedy:

$$(g_1, g_2, \dots) * (h_1, h_2, \dots) = (g_1 *_1 h_1, g_2 *_2 h_2, \dots). \quad (6.2)$$

Je zřejmé, že výsledkem přímého součinu grup je opět grupa a to řádu $|G| = |G_1||G_2| \dots |G_n|$ nebo nekonečného.

6.1 Klasifikace Abelovských grup

Definice 6.2. 1. Grupa G je **konečně generovaná**, pokud existuje konečná množina $A \subset G$ taková, že $G = \langle A \rangle$.

2. Pro každé $r \in \mathbb{Z}$, $r \geq 0$, buď $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ direktní součet r kopií grupy $\mathbb{Z}$, kde $\mathbb{Z}^0 = e$. Grupa $\mathbb{Z}^r$ se nazývá **volná Abelovská grupa řádu r** .

Věta 6.3 (základní věta Abelovských grup). *Buď G konečně generovaná Abelovská grupa. Pak:*

1. $G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \dots \times Z_{n_s}$ pro nějaká celá čísla splňující následující podmínky:
 - a) $r \geq 0$ a $n_j \geq 2$ pro všechna j ,
 - b) $n_{i+1} | n_i$ pro $1 \leq i \leq s-1$,
2. a rozklad je jednoznačný.

Důkaz. Bez důkazu. □

POZNÁMKA 6.4. Každý prvočíselný dělitel $|G|$ musí dělit n_1 .

Věta 6.5. *Buď G grupa řádu $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Potom*

1. $G \cong A_1 \times A_2 \times \dots \times A_k$, kde $|A_i| = p_i^{\alpha_i}$,

6 Přímý a polopřímý součin grup

2. pro každé $A \in A_1, A_2, \dots, A_k$, kde $|A| = p^\alpha$ je $A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \dots \times Z_{p^{\beta_t}}$, kde $\beta_1 \geq \beta_2 \geq \dots \geq \beta_t \geq 1$ a $\beta_1 + \beta_2 + \dots + \beta_t = \alpha$ (t a β_j závisí na i)

3. a rozklad v 1) a 2) je jednoznačný až na pořadí A_i .

Důkaz. Bez důkazu. □

Věta 6.6. Necht $m, n \in \mathbb{Z}^+$, pak $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Leftrightarrow \gcd(m, n) = 1$ (tj. m a n jsou nesoudělná).

Důkaz. $\Rightarrow$) Necht $\mathbb{Z}_m = \langle x \rangle$, $\mathbb{Z}_n = \langle y \rangle$ a $l = \text{lcm}(m, n)$ (nejmenší společný násobek). Všimneme si, že $l = mn$, právě když $\gcd(m, n) = 1$. Dále necht $x^a y^b \in \mathbb{Z}_m \times \mathbb{Z}_n$ libovolné, pak

$$(x^a y^b)^l = x^{la} y^{lb} = e^a e^b = e,$$

protože $m \mid l$ a taky $n \mid l$. Pokud $\gcd(m, n) \neq 1$, každý element $\mathbb{Z}_m \times \mathbb{Z}_n$ je řádu nanejvýš l , tedy ostře menšího než mn , tedy $\mathbb{Z}_m \times \mathbb{Z}_n$ nemůže být isomorfní $\mathbb{Z}_{mn}$.

$\Leftarrow$) Naopak, pokud $\gcd(m, n) = 1$, pak $|xy| = \text{lcm}(|x|, |y|) = mn$. Tudíž $\mathbb{Z}_m \times \mathbb{Z}_n = \langle xy \rangle$. □

Věta 6.7. Necht $H, K \leq G$. Počet různých způsobů, jak napsat libovolný element z HK ve tvaru hk pro nějaké $h \in H$ a $k \in K$, je $|H \cap K|$. Speciálně když $H \cap K = e$, pak pro každý element existuje pouze jeden způsob.

Důkaz. Necht $x \in HK$ a $y \in H \cap K$ libovolné, pak $x = yy^{-1}x = yz$, kde $z = y^{-1}x$ je element H nebo K . Takže existuje alespoň $|H \cap K|$ možností, jak zvolit y . Kdyby existovalo $x \in HK$, které lze zapsat více různými způsoby než $H \cap K$, pak celkový počet způsobů, jak zapsat všechny prvky, by byl větší než

$$|HK||H \cap K| = \frac{|H||K|}{|H \cap K|}|H \cap K| = |H||K|,$$

což je spor s růzností zápisu. □

Věta 6.8. Necht $H, K \trianglelefteq G$ a $H \cap K = e$, pak $HK \cong H \times K$.

Důkaz. Protože $H, K \trianglelefteq G$, je $HK \leq G$. Necht $h \in H$, $k \in K$. Protože $H \trianglelefteq G$, platí $k^{-1}hk \in H$, tedy taky $h^{-1}(k^{-1}hk) \in H$. Analogicky, $(h^{-1}k^{-1}h)k \in K$. Dále díky tomu, že $H \cap K = e$, máme $h^{-1}k^{-1}hk = e$, tedy $hk = kh$, takže prvky H komutují s prvky K . Podle předcházející věty lze každý prvek HK zapsat právě jedním způsobem ve tvaru hk , kde $h \in H$ a $k \in K$. Zobrazení

$$\varphi : HK \rightarrow H \times K : hk \rightarrow (h, k)$$

je proto dobře definované. Pro důkaz toho, že φ je homomorfismus, vezměme $h_1, h_2 \in H$ a $k_1, k_2 \in K$. Pak díky tomu, že prvky H a K spolu komutují, platí

$$(h_1 k_1)(h_2 k_2) = (h_1 h_2)(k_1 k_2)$$

a tento tvar je jednoznačně zapsán ve tvaru hk , kde $h \in H$, $k \in K$. Takže

$$\varphi(h_1 k_1 h_2 k_2) = \varphi(H_1 h_2 k_1 k_2) = (h_1 h_2, k_1 k_2) = (h_1, k_1)(h_2, k_2) = \varphi(h_1 k_1) \varphi(h_2 k_2),$$

tedy φ je homomorfismus. Zároveň je to ale bijekce, proto φ je isomorfismus. □

6.2 Polopřímý součin

POZNÁMKA 6.9. Polopřímý součin je další způsob, jak z menších grup vyrobit grupu větší. Ve výsledku dostaneme z grup H a K grupu G , ve které bude platit $H \trianglelefteq G$, ale $K \leq G$ nemusí být normální. Jako motivaci předpokládejme, že už takovou G máme a platí $H \cap K = e$. Platí, že $HK \leq G$ a existuje bijekce mezi prvky HK a dvojicemi (h, k) , kde $h \in H$ a $k \in K$. Chceme-li součin dvou prvků z HK opět napsat ve tvaru hk , postupujeme takto:

$$(h_1 k_1)(h_2 k_2) = h_1 k_1 h_2 (k_1^{-1} k_1) k_2 = h_1 (k_1 h_2 k_1^{-1}) k_1 k_2 = h_1 h_3 k_3 = h_4 k_3,$$

kde jsme využili toho, že H je normální podgrupa. Cílem polopřímého součinu je zavést grupu s obdobným násobením bez „zastřešující“ grupy, která nám umožňuje násobit mezi sebou prvky z K a H .

Věta 6.10. *Bud' H a K grupy a $\varphi : K \rightarrow \text{Aut } H$ je homomorfismus (každému prvku $k \in K$ přiřadí nějakou permutaci H). Dále bud' akce grupy K na H daná vztahem $\varphi(k)h = k \cdot h$. Bud' G množina dvojic (h, k) , $h \in H$ a $k \in K$ a definuje násobení těchto dvojic jako:*

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2).$$

1. G s takto definovanou operací je grupa řádu $|G| = |K||H|$.
2. Množiny $\{(h, 1) | h \in H\}$ a $\{(1, k) | k \in K\}$ jsou podgrupy G isomorfní grupám H a K . (Dále mezi nimi nerozlišujeme.)
3. $H \trianglelefteq G$.
4. $H \cap K = e$.
5. $(\forall h \in H, k \in K)(khk^{-1} = k \cdot h)$.

Důkaz. 1. Asociativita platí, protože pro libovolné $(a, x), (b, y), (c, z) \in G$ platí

$$\begin{aligned} ((a, x)(b, y))(c, z) &= (ax \cdot b, xy)(c, z) \\ &= (ax \cdot b(xy) \cdot c, xyz) \\ &= (ax \cdot bx \cdot (y \cdot c), xyz) \\ &= (ax \cdot (by \cdot c), xyz) \\ &= (a, x)(by \cdot c, yz) \\ &= (a, x)((b, y)(c, z)). \end{aligned}$$

Platnost rovnosti mezi řádky 3 a 4 odpovídá axiomu homomorfismu $\varphi(b)\varphi(y \cdot c) = \varphi(b(y \cdot c))$. Dále je z definice vidět, že $(1, 1)$ je jednotkový prvek, $(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$ je inverzní prvek pro libovolné $(h, k) \in G$ a $|G| = |H||K|$.

2. Nechť $\tilde{H} = \{(h, 1) | h \in H\}$ a $\tilde{K} = \{(1, k) | k \in K\}$. Máme

$$(a, 1)(b, 1) = (a1 \cdot b, 1) = (ab, 1), \quad \forall a, b \in H.$$

Analogicky,

$$(1, x)(1, y) = (1, xy), \quad \forall x, y \in K,$$

takže $\tilde{H}, \tilde{K} \leq G$ isomorfní H, K .

6 Přímý a polopřímý součin grup

4. Je jasné, že $\tilde{H} \cap \tilde{K} = e$.

5. Dále platí

$$\begin{aligned} (1, k)(h, 1)(1, k)^{-1} &= ((1, k)(h, 1))(1, k^{-1}) \\ &= (k \cdot h, k)(1, k^{-1}) \\ &= (k \cdot hk \cdot 1, kk^{-1}) \\ &= (k \cdot h, 1), \end{aligned}$$

tedy přiřazením $h \leftrightarrow (h, 1)$ a $k \leftrightarrow (1, k)$ z bodu (2.) dostáváme $khk^{-1} = k \cdot h$.

3. Nakonec, protože $K \leq N_G(H)$, platí $G = HK$ a zároveň $H \leq N_G(H)$, dostáváme $N_G(H) = G$, tedy $H \trianglelefteq G$.

□

Definice 6.11. Grupy G z předchozí věty nazýváme **polopřímý součin** grup H a K a značíme $H \rtimes_{\varphi} K$.

7 Reprezentace grup

$$GL(V) = \{ L \in \mathcal{L}(V) \mid \ker L = \{0\} \}$$

tj. neregulární

7.1 Základní definice

Definice 7.1. Buďte G grupa a V vektorový prostor nad tělesem T . Potom **lineární reprezentací** grupy G na prostoru V nazýváme každý homomorfismus $T : G \rightarrow GL(V)$, který každému prvku $g \in G$ přiřazuje lineární zobrazení $T(g)$ takové, že $(\forall g, h \in G)(T(g)T(h) = T(gh))$.

- Prostor V nazýváme **reprezentativní prostor** a jeho dimenzi **rozměr** reprezentace.
- Je-li navíc T isomorfismus, nazýváme takovou reprezentaci **věrná**. *isomorfismus na $M \leq GL(V)$*
- Je-li $\dim V < \infty$ (existuje tedy konečná báze V), mluvíme o **maticové** reprezentaci.

POZNÁMKA 7.2. • T je vždy věrnou reprezentací faktor grupy $G/\text{Ker } T$.

- Prostá grupa má jen věrné reprezentace (kromě triviální). *není normální podgrupa*

Definice 7.3. Je-li $\mathcal{H}$ Hilbertův prostor a T homomorfismus grupy G do množiny unitárních operátorů na $\mathcal{H}$, nazýváme T **unitární** reprezentací G na $\mathcal{H}$.

nelze faktorizovat

Definice 7.4. Dvě reprezentace $T : G \rightarrow V$ a $T' : G \rightarrow V'$ nazýváme **ekvivalentní**, pokud existuje lineární isometrie $A : V \rightarrow V'$ taková, že $\forall g \in G$ platí $T'(g) = AT(g)A^{-1}$ a $\|A\varphi\| = \|\varphi\|$, $\forall \varphi \in V$. Je-li navíc A unitární, říkáme, že reprezentace jsou **unitárně ekvivalentní**.

it. $\|A\|=1$

Lemma 7.5 (Hilbert). *Každá maticová reprezentace grupy je ekvivalentní unitární reprezentaci.*

Důkaz. Konstrukcí: Buď A_i matice reprezentující prvek $g_i \in G$. Sestrojíme nejprve hermitovskou matici $H = \sum_{i=1}^{|G|} A_i A_i^\dagger$. Hermitovské matice můžeme diagonalizovat pomocí unitární matice U . Nechť tato diagonalizovaná matice je:

$$D = U^{-1} H U = \sum_i^{|G|} U^{-1} A_i A_i^\dagger U = \sum_i U^{-1} A_i U U^{-1} A_i^\dagger U = \sum_i A'_i A_i'^\dagger,$$

kde jsme označili $A'_i = U^{-1} A_i U$. Rozpisem poslední sumy

$$\sum_i A'_i A_i'^\dagger = \sum_i \sum_j (A'_i)_{kj} (A_i'^\dagger)_{jk} = \sum_i \sum_j |(A'_i)_{kj}|^2$$

zjišťujeme, že diagonální členy D jsou kladné, protože jednou z matic A'_i je identita (člen $j = k$). Proto můžeme vytvořit matice $D^{\frac{1}{2}}$ a $D^{-\frac{1}{2}}$. Potom z definice zřejmě platí:

$$I = D^{-\frac{1}{2}} \sum_i A'_i A_i'^\dagger D^{-\frac{1}{2}}.$$

$$A'' = D^{-1/2} U^\dagger A U D^{1/2}$$

7 Reprezentace grup

Nyní již definujeme matice finální reprezentace $A_i'' = D^{-1/2} A_i' D^{1/2}$, o kterých ukážeme, že jsou unitární:

$$\begin{aligned} A_j'' A_j''^\dagger &= D^{-1/2} A_j' D^{1/2} I D^{1/2} A_j'^\dagger D^{-1/2} = \\ &= D^{-1/2} A_j' D^{1/2} D^{-1/2} \sum_i A_i' A_i'^\dagger D^{-1/2} D^{1/2} A_j'^\dagger D^{-1/2} = \\ &= D^{-1/2} \sum_i A_j' A_i' (A_j' A_i')^\dagger D^{-1/2} = \\ &= D^{-1/2} \sum_k A_k' A_k'^\dagger D^{-1/2} = I. \end{aligned}$$

Tím je důkaz dokončen. $\square$

7.2 Reducibilní a ireducibilní reprezentace

Definice 7.6. $V_1 \subset V$ se nazývá **invariantní** podprostor příslušný operátoru A , když $(\forall \varphi \in V_1)(A\varphi \in V_1)$, tedy $A(V_1) \subset V_1$. Pokud se nejedná o triviální invariantní podprostor, nazývá se takový podprostor **vlastní**.

Definice 7.7. Říkáme, že T je **ireducibilní** reprezentace grupy G na prostoru V , pokud neexistuje vlastní invariantní podprostor V příslušný všem operátorům $T(g)$ pro všechna $g \in G$. Tedy $(\forall g \in G)(T(g)(V_1) \subset V_1) \Rightarrow (V_1 = 0 \vee V_1 = V)$. V opačném případě se reprezentace nazývá **reducibilní**.

POZNÁMKA 7.8. Reprezentace je ireducibilní, pokud neexistuje taková podobnostní transformace, která by převedla současně všechny $T(g)$ na blokově diagonální tvar.

Definice 7.9. Reducibilní reprezentace, kterou je možné napsat jako direktní součet ireducibilních reprezentací se nazývá **úplně reducibilní**.

Věta 7.10. Bud' T unitární reprezentace grupy G na Hilbertově prostoru $\mathcal{H}$. Potom:

1. Ortogonální doplněk k $\mathcal{H}_1$ (označme $\mathcal{H}_2$) je invariantní podprostor $\Leftrightarrow \mathcal{H}_1$ je invariantní podprostor.
2. $\mathcal{H}_1 \subset \mathcal{H}$ je invariantní podprostor $\Leftrightarrow$ projektor E_1 na $\mathcal{H}_1$ splňuje podmínku: $(T(g)E_1 = E_1T(g))(\forall g \in G)$.

Důkaz. 1. Nechť $\psi_1 \in \mathcal{H}_1$ a $\psi_2 \in \mathcal{H}_2$, pak z předpokladu máme $T(g)|\psi_1\rangle \in \mathcal{H}_1 = \mathcal{H}_2^\perp$ a platí

$$\langle \psi_2 | T(g) \psi_1 \rangle = 0 = \langle T(g)^\dagger \psi_2 | \psi_1 \rangle. = \langle T(g^{-1}) \psi_2 | \psi_1 \rangle \quad (7.1)$$

2. Můžeme psát $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$, tedy $\forall |\psi\rangle \in \mathcal{H}$ platí $|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle$, kde $|\psi_1\rangle \in \mathcal{H}_1$ a $|\psi_2\rangle \in \mathcal{H}_2$.

$\Rightarrow$) Předpokládáme, že $\mathcal{H}_1$, a z předchozího bodu též $\mathcal{H}_2$, jsou invariantní.

$$E_1 T(g) |\psi\rangle = E_1 T(g) |\psi_1\rangle + \overbrace{E_1 T(g) |\psi_2\rangle}^{= T(g) \psi_2} = E_1 T(g) E_1 |\psi\rangle = T(g) E_1 |\psi\rangle. \quad (7.2)$$

$\Leftarrow$) Z rovnosti $E_1 T(g) |\psi\rangle = T(g) E_1 |\psi\rangle$ plyne že $T(g) \mathcal{H}_1 \subset \mathcal{H}_1$.

□

Důsledek 7.11 (Maschke). *Reducibilní unitární reprezentace je úplně reducibilní.*

Věta 7.12. *Každá unitární ireducibilní reprezentace konečné grupy má konečnou dimenzi.*

Důkaz. Bez důkazu. □

7.2.1 Schurova lemmata

Věta 7.13 (1. Schurovo lemma). *Každá matice, která komutuje se všemi maticemi ireducibilní reprezentace je násobkem jednotkové matice.*

Důkaz. Víme, že se můžeme omezit je na unitární matice. Mějme tedy matici M , pro kterou platí $MA_i = A_iM$ pro $\forall i$. Sdružením obou stran dostaneme $M^\dagger A_i^\dagger = A_i^\dagger M^\dagger$ a vynásobením maticí A_i zprava i zleva dostaneme $A_i M^\dagger = M^\dagger A_i$, tedy i $M^\dagger$ komutuje se všemi maticemi reprezentace. Nyní můžeme vytvořit hermitovské matice $H_1 = M + M^\dagger$ a $H_2 = i(M - M^\dagger)$ a vyjádřit $M = H_1 - iH_2$. Potom M je konstantní právě tehdy, když tyto hermitovské matice jsou konstantní, a proto se můžeme omezit na hermitovské komutující matice.

Hermitovskou matici můžeme diagonalizovat, tedy $D = U^{-1}MU$ a definujeme $A'_i = U^{-1}A_iU$. Potom platí $A'_i D = D A'_i$ díky invarianci maticových rovnic vůči unitárním transformacím. Nyní musíme ukázat, že D je nejen diagonální, ale přímo násobkem jednotkové matice. Napíšeme po složkách $(A'_i)_{\mu\nu} d_{\nu\nu} = d_{\mu\mu} (A'_i)_{\mu\nu}$, tedy $(A'_i)_{\mu\nu} (d_{\nu\nu} - d_{\mu\mu}) = 0$. Pokud by pro nějaké $\mu\nu$ bylo $(d_{\nu\nu} - d_{\mu\mu}) \neq 0$, muselo by být $(A'_i)_{\mu\nu} = 0$ pro $\forall i$, což je spor s ireducibilitou reprezentace. Odtud dostáváme $d_{\nu\nu} = d_{\mu\mu}$ pro $\forall \mu\nu$. □

Věta 7.14 (2. Schurovo lemma). *Máme-li dvě ireducibilní reprezentace T_1 a T_2 rozměru l_1 a l_2 jedné grupy G a dále existuje obdélníková matice M , pro kterou platí: $MT_1(g) = T_2(g)M$ pro $\forall g \in G$, pak*

1. $(l_1 \neq l_2) \Rightarrow M = 0$ (nulová matice)
2. a pro $l_1 = l_2$ je buď $M = 0$, nebo $\det M \neq 0$, a tedy existuje M^{-1} , z čehož dostáváme $MT_1(g)M^{-1} = T_2(g)$ pro $\forall g \in G$, a tedy obě reprezentace jsou ekvivalentní.

Důkaz. Opět uvažujeme pouze unitární matice a bez újmy na obecnosti nechť $l_1 \leq l_2$. Nyní sdružením rovnice pro M dostaneme: $T_1(g)^\dagger M^\dagger = M^\dagger T_2(g)^\dagger$, neboli $T_1(g^{-1})M^\dagger = M^\dagger T_2(g^{-1})$. Nyní obě strany vynásobíme M a využijeme toho, že rovnost platí pro všechny g_i^{-1} stejně jako pro všechna g_i . Dostaneme (použitím základní rovnosti)

$$T_2(g_i^{-1})MM^\dagger = MM^\dagger T_2(g_i^{-1}).$$

Tedy matice $MM^\dagger$ komutuje se všemi maticemi reprezentace a podle předchozího lemmatu musí platit $MM^\dagger = cI$.

Uvažujme nejprve $l_1 = l_2$, tedy M je čtvercová matice. Pomocí pravidel počítání determinantů máme $(\det M)^2 = c^l$. Nyní pokud $c \neq 0$, musí mít M nenulový determinant. V případě, že $c = 0$ máme $MM^\dagger = 0$. Po složkách tedy $\sum_\alpha M_{\mu\alpha} M_{\nu\alpha}^* = 0$ pro $\forall \mu\nu$. Speciálně volbou $\mu = \nu$ dostáváme $\sum_\alpha |M_{\mu\alpha}|^2 = 0$, a tedy $M_{\mu\alpha} = 0$ pro $\forall \mu\alpha$.

V případě, že $l_1 < l_2$, tedy M má l_1 sloupců a l_2 řádků, doplní M přidáním $l_2 - l_1$ sloupců na čtvercovou matici N . Platí, že $NN^\dagger = MM^\dagger$. Jelikož N má zřejmě nulový determinant, dostáváme případ, kdy $M = 0$. □

7.3 Velká věta ortogonality

Věta 7.15 (velká věta ortogonality). *Uvažujme všechny neekvivalentní ireducibilní unitární reprezentace grupy G . Platí:*

$$\sum_{g \in G} T_i(g)_{\mu\nu}^* T_j(g)_{\alpha\beta} = \frac{|G|}{l_i} \delta_{ij} \delta_{\mu\alpha} \delta_{\nu\beta}, \quad (7.3)$$

kde l_i je rozměr reprezentace T_i .

Důkaz. Nejprve uvažujeme dvě neekvivalentní reprezentace T_1 a T_2 . Zkonstruujeme matici:

$$M = \sum_g T_2(g) X T_1(g^{-1}),$$

kde X je zatím zcela libovolná obdélníková matice, která odpovídá rozměrem. Nyní použijeme větu 7.14, a proto ukážeme potřebnou rovnost:

$$\begin{aligned} T_2(f)M &= \sum_g T_2(f)T_2(g)XT_1(g^{-1}) = \\ &= \sum_g T_2(f)T_2(g)XT_1(g^{-1})T_1(f^{-1})T_1(f) = \\ &= \sum_g T_2(fg)XT_1(g^{-1}f^{-1})T_1(f) = \\ &= \sum_g T_2(fg)XT_1((fg)^{-1})T_1(f) = \\ &= \sum_h T_2(h)XT_1(h^{-1})T_1(f) = MT_1(f). \end{aligned} \quad (7.4)$$

Musí tedy platit, že $M = 0$, tedy

$$M_{\alpha\mu} = 0 = \sum_g \sum_{\kappa\lambda} T_2(g)_{\alpha\kappa} X_{\kappa\lambda} T_1(g^{-1})_{\lambda\mu}. \quad (7.5)$$

Nyní si zvolíme konkrétní matici X a to tak, že $X_{\beta\nu} = 1$ (jeden prvek je jedna) a ostatní prvky jsou nulové. Pak předchozí rovnost dává:

$$0 = \sum_g T_2(g)_{\alpha\beta} T_1(g^{-1})_{\nu\mu} = \sum_g T_2(g)_{\alpha\beta} T_1(g)_{\mu\nu}^*, \quad (7.6)$$

kde poslední úprava je z unitarity matice. To nám tedy dává člen δ_{ij} ve výsledku (pro různé reprezentace je skalární součin vždy 0).

Nyní mějme jednu reprezentaci a znovu zkonstruujeme matici M jako:

$$M = \sum_g T_1(g) X T_1(g^{-1}),$$

7 Reprezentace grup

a ze Schurova lemmatu máme $M = cI$. Vezměme prvek $\mu\mu'$, což nám dá rovnici:

$$\sum_g \sum_{\kappa\lambda} T_1(g)_{\mu\kappa} X_{\kappa\lambda} T_1(g^{-1})_{\lambda\mu'} = c\delta_{\mu\mu'}.$$

Opět zvolíme X jen s jedním nenulovým prvkem $X_{\nu\nu'} = 1$. Potom:

$$\sum_g T_1(g)_{\mu\nu} T_1(g^{-1})_{\nu'\mu'} = c_{\nu\nu'} \delta_{\mu\mu'},$$

kde indexy u c značí, že jeho hodnota závisí na volbě matice X . Nyní zvolíme $\mu = \mu'$ a sečteme přes μ .

$$\begin{aligned} \sum_g T_1(gg^{-1})_{\nu'\nu} &= l_1 c_{\nu\nu'}, \\ \sum_g T_1(gg^{-1})_{\nu'\nu} &= \sum_g T_1(e)_{\nu'\nu} = |G| \delta_{\nu\nu'}. \end{aligned}$$

Odtud máme $c_{\nu\nu'} = \frac{|G|\delta_{\nu\nu'}}{l_1}$. Zpětným dosazením za c dostaneme:

$$\sum_g T_1(g)_{\mu\nu} T_1(g^{-1})_{\nu'\mu'} = \frac{|G|}{l_1} \delta_{\nu\nu'} \delta_{\mu\mu'} = \sum_g T_1(g)_{\mu\nu} T_1(g)_{\mu'\nu'}^*,$$

což dokazuje tvrzení věty. □

POZNÁMKA 7.16. Velká věta ortogonality tedy říká, že pokud vytvoříme vektory čísel o počtu prvků $|G|$ tak, že si zvolíme jednu reprezentaci a v ní μ -tý řádek a ν -tý sloupec a prvky vektoru jsou prvky matice reprezentace pro jednotlivé prvky grupy G , pak jsou tyto vektory vzájemně kolmé pro různé reprezentace nebo různé pozice v matici. (Musíme mít stanovené pořadí prvků v G .) Označme $|G| = n$. Vektory s n prvky tvoří n -dimenzionální vektorový prostor. V takovém prostoru tedy může být maximálně n vzájemně kolmých vektorů, a proto platí, že $\sum_i l_i^2 \leq n$, kde suma jde přes všechny neekvivalentní ireducibilní reprezentace. (Později se zde ukáže, že vždy platí rovnost.)

7.4 Tabulky charakterů

POZNÁMKA 7.17. Pro maticové reprezentace zavedeme užitečnou veličinu nezáviselou na bázi – tzv. charakter reprezentace.

Definice 7.18. Označme stopu $\text{Tr}(T(g)) = \chi(g)$. Uspořádanou n -tici stop matic $T(g)$ nazveme **charakter** reprezentace.

POZNÁMKA 7.19. Charaktery ekvivalentních reprezentací jsou zřejmě stejné.

Tvrzení 7.20. Velká věta ortogonality pro charaktery prvků grupy:

$$\sum_{g \in G} \chi^{(\mu)}(g)^* \chi^{(\nu)}(g) = n \delta_{\mu\nu}. \quad (7.7)$$

POZNÁMKA 7.21. Charaktery všech konjugovaných prvků grupy jsou stejné.

7 Reprezentace grup

Tvrzení 7.22. *Velká věta ortogonalit pro charaktery konjugovaných prvků grupy:*

$$\sum_i n_i \chi^{(\mu)}(C_i)^* \chi^{(\nu)}(C_i) = n \delta_{\nu\mu}, \quad (7.8)$$

kde $G = C_1 \cup \dots \cup C_k$ a n_i je počet prvků v konjugované třídě. Prvky

$$\chi'^{(\mu)}(C_i) = \sqrt{\frac{n_i}{n}} \chi^{(\mu)}(C_i) \quad (7.9)$$

tvorí ortonormální systém, který je větší nebo roven počtu neekvivalentních reprezentací.

Věta 7.23. *Mějme unitární reducibilní reprezentaci $T(g)$ rozepsanou pomocí ireducibilních reprezentací jako $T(g) = \bigoplus_{\nu} a_{\nu} T^{(\nu)}(g)$. Označme $\chi(C_i) = \sum_{\nu} a_{\nu} \chi^{(\nu)}(C_i)$. Potom pro koeficienty rozkladu a_{μ} platí*

$$a_{\mu} = \frac{1}{n} \sum_i n_i \chi^{(\mu)}(C_i)^* \chi(C_i). \quad (7.10)$$

Důkaz. Rovnost $\chi(C_i) = \sum_{\nu} a_{\nu} \chi^{(\nu)}(C_i)$ vynásobme $n_i \chi^{(\mu)}(C_i)$ a vysčítáme přes i . □

Důsledek 7.24. *Z definice je $T(g)$ ireducibilní transformace, právě když $a_{\mu} = 1$. Poté platí*

$$\sum_i \chi^{(\mu)}(g_i)^* \chi(g_i) = n. \quad (7.11)$$

Tomuto vztahu se říká Frobeniova podmínka.

Literatura

- [1] David S. Dummit, Richard M. Foote *Abstract Algebra*, 2003.