

Grupy a reprezentace

Goce Chadzitaskos

Zpracováno na základě poznámek J. Mareše a s jejich využitím

wiki-skripta

Systémy, které studujeme v přírodě, vykazují určitý druh symetrie, a řada přírodních zákonů, které známe, je invariantní vůči jistým transformacím.

Vzpomeňte: teorém Noetherové, Gaussův a Ampérův zákon, Lorentzovy transformace, krystalické mřížky.

Množina všech možných transformací určité symetrie vytváří to, co matematici nazývají „grupa“. Tak zrcadlení v rovině vytváří grupu, která má dva prvky: zrcadlení a identitu. Ale také množina trojrozměrných rotací, množina Lorentzových transformací nebo množina trojrozměrných translací jsou grupy, které ale nyní sestávají z nekonečného množství prvků.

- Évariste Galois (1832): kdy má obecný polynom radikálové řešení - kdy je možno kořeny zapsat jen s užitím základních aritmetických operací a odmocnin - všechny permutace, které nemějí $I_1, I_2, \dots, I_n$
- Sophus Lie (1888) : Symetrie parciálních diferenciálních rovnic - spojitá symetrie
- H Weyl: Symetrie je jedna z myšlenek, díky níž se lidé během věků snaží pochopit a tvořit řád, krásu a dokonalost.
- Michelangelo di Lodovico Buonarroti: Malá asymetrie oku lahodí
- obrazy Salvatora Dalího
- kvantová mechanika: Ireducibilní reprezentace (IRR) grupy symetrie na Hilbertově prostoru.
- obecná Fourierova transformace: pomocí IR je definována ortogonální báze na prostoru

Ze zřejmých důvodů se grupy s konečným počtem prvků nazývají diskrétní; grupy transformací, které spojitě závisí na řadě parametrů se nazývají spojitě grupy.

Symetrie systému vede k určitým vztahům mezi pozorovatelnými veličinami, které jsou splněny s nekonečně vysokou přesností, Symetrie SU(2) je zodpovědná za kvantování momentu setrvačnosti - je to dáno ireducibilními reprezentacemi.

Další hezký příklad této symetrie pro částicové fyziky jsou rodiny částic (isospin) a jejich rozpady

Příklad pro rozpad baryonové resonance na nukleon a pion

$$\Delta^{++} \rightarrow p\pi^{+}$$

$$\Delta^{+} \rightarrow p\pi^{0} \text{ or } \rightarrow n\pi^{+}$$

$$\Delta^{0} \rightarrow n\pi^{0} \text{ or } \rightarrow p\pi^{-}$$

$$\Delta^{-} \rightarrow n\pi^{-}$$

Using the common names in particle physics, one assigns the isospin states as follows: The triplet of π mesons π^{+} , π^{0} , π^{-} respectively as $|\frac{2}{2}\rangle$, $|\frac{2}{0}\rangle$, $|\frac{2}{-2}\rangle$; the doublet of nucleons p and n respectively as $|\frac{1}{1}\rangle$ and $|\frac{1}{-1}\rangle$ and the quadruplet of resonances Δ^{++} , Δ^{+} , Δ^{0} and Δ^{-} with $|\frac{3}{3}\rangle$, $|\frac{3}{1}\rangle$, $|\frac{3}{-1}\rangle$ and $|\frac{3}{-3}\rangle$

Rozpadové schéma pro rezonance

$$|\frac{3}{3}\rangle = |\frac{2}{2}\rangle|\frac{1}{1}\rangle$$

$$|\frac{3}{1}\rangle = |\frac{2}{0}\rangle|\frac{1}{1}\rangle \text{ or } |\frac{2}{2}\rangle|\frac{1}{-1}\rangle$$

$$|\frac{3}{-1}\rangle = |\frac{2}{0}\rangle|\frac{1}{-1}\rangle \text{ or } |\frac{2}{-2}\rangle|\frac{1}{1}\rangle$$

$$|\frac{3}{-3}\rangle = |\frac{2}{-2}\rangle|\frac{1}{-1}\rangle$$

- $\Delta^{++} \rightarrow p\pi^+$ is 1
- $\Delta^+ \rightarrow p\pi^0$ is $\frac{2}{3}$ and $\Delta^+ \rightarrow n\pi^+$ is $\frac{1}{3}$
- $\Delta^0 \rightarrow n\pi^0$ is $\frac{2}{3}$ and $\Delta^0 \rightarrow p\pi^-$ is $\frac{1}{3}$
- $\Delta^- \rightarrow n\pi^-$ is 1

Mějme libovolnou množinu M .

Def: Potom **n -ární operací** na M nazveme zobrazení

$$f : \underbrace{M \times M \times \dots \times M}_n \rightarrow M.$$

*Operaci $f : M \times M \rightarrow M$ (binární operace) budeme nazývat **vnitřní součin** a místo $f(x, y) = z$ ji budeme značit $x \cdot y = z$, nebo $x \times y = z$, nebo $x + y = z$, podle potřeby.*

Neplést vnitřní součin s pojmem skalární součin (angl.: scalar product = inner product). Příkladem binární operace na vektorovém prostoru je vektorový součin vektorů. Výsledek skalárního součinu nepatří do množiny M .

Grupoid, Pologrupa = asociativita

Nejobecnější objekt je dvojice množina a vnitřní součin

- ① $\{M, \cdot\}$ nazýváme **grupoid**.

Dále při splnění dodatečných podmínek zavádíme:

- ② $(\forall a, b, c \in M)((ab)c = a(bc))$: **pologrupa** (asociativní grupoid),
- ③ $(\forall a, b \in M)(ab = ba)$: **komutativní grupoid**,
- ④ je-li počet prvků M konečný: **konečný grupoid**.

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

Monoid = asociativita + jednotka

Theorem

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

Důkaz.

$$e_l = e_l e_p = e_p$$



- 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 asociivitě 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} .)

Theorem

Každý prvek monoidu má nejvýše jeden inverzní prvek.

Důkaz.

Nechť $f, g, m \in M$ a platí $fm = e$ a $gm = e$, pak $f = ef = (gm)f = g(mf) = ge = g$. Využíváme pouze asociativitu. □

Zavádíme:

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

Grupa = asociativita + jednotka + $\exists$ inverzního

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

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 $(\forall m \in M)(\exists m^{-1} \in M)(mm^{-1} = e).$

A tímto způsobem bývá též definována.

Example

- 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 $a \oplus_{\text{modulo } p} b \equiv a + b \pmod{p}$, (značená $\mathbb{Z}_p \equiv \mathbb{Z}/p\mathbb{Z}$),
- 3 množina kvaternionů s násobením.

Example

Dalším příkladem grupy je množina $\mathbb{Q}[\sqrt{p}] = \{m + n\sqrt{p} \mid m, n \in \mathbb{Q}\}$ 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:

$$a \cdot b = (a_1 + a_2\sqrt{p})(b_1 + b_2\sqrt{p}) = a_1b_1 + a_2b_1\sqrt{p} + a_1b_2\sqrt{p} + a_2b_2p.$$

*Komutativní grupu nazýváme **abelovská**.*

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

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

Značku 0 používáme pro jednotkový prvek vůči operaci značené $\oplus$ a značku 1 pro jednotkový prvek vůči operaci značené $\odot$ nebo $\otimes$ díky analogii s $\mathbb{R}$.

H. Weyl: *Těleso je uzavřený vesmír, kde probíhají všechny děje.*

Vektorový prostor (nad tělesem)

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 $(\forall x \in M)(0 \times x = 0).$

Též **lineární prostor**

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

- 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 $\mathbb{T}$.

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

Speciální a důležitou skupinou jsou topologické grupy:

*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 $g(x) = x^{-1}$ spojité.*

Topologie: Množina a systém otevřených podmnožin $(M, \mathcal{O})$ s vlastnostmi:

- 1 $\emptyset \in \mathcal{O}, M \in \mathcal{O}$
- 2 $\cap_1^n \in \mathcal{O}, n < \infty$
- 3 $\cup_1^n \in \mathcal{O}, n \leq \infty$

Triviální - pouze $\emptyset \in \mathcal{O}$ a $M \in \mathcal{O}$, diskrétní - všechny podmnožiny.

Spojitosť v $\mathbb{R}$

Jednoduchý příklad: Kleinova grupa

Example

Mějme grupu $G = (\{e, a, b\}, \odot) \cong \mathbb{Z}_3 = (\{0, 1, 2\}, +_{\text{mod}3})$. 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.

Homogenní prostor

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

Theorem

Každá topologická grupa je homogenní topologický prostor.

Důkaz.

Pro $\forall x, y \in G, \exists! a = yx^{-1}$. Určitě platí $a \in G$ a $ax = yx^{-1}x = y$. Hledaný homeomorfismus tedy bude $f(x) = ax$ (spojitost operací v topologické grupě).



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

Proto stačí vyšetřovat topologické grupy v okolí a zobrazením lze roztáhnout po celém prostoru.

$$g(U_e) = U_g,$$

zobrazení g^{-1} je spojité.

*Topologické grupa G se nazývá **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 .

Theorem

Hilbert, Pontryagin von Neumann Každá parametrická grupa je Lieova grupa, pokud ϕ a $\phi \circ \psi^{-1}$ jsou analytické.

Toto zúžení je přechod od abstraktních topologických grup k matematické analýze díky souřadnicím.

Example

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 $\{x_{i,j}\}_{i,j=1}^n$.

Násobení matic dá $\mathbb{I} + \tilde{z} = (\mathbb{I} + \tilde{x})(\mathbb{I} + \tilde{y})$ a $\tilde{z} = \tilde{x} + \tilde{y} + \tilde{x}\tilde{y}$.

Pozn.

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).

Definujeme

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.)

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

Pro každý $g \in G$ platí $|g| \leq |G|$. Pro nekonečný řád grupy to platí triviálně, pro konečnou grupu platí následující argument:

Vezmeme posloupnost $\{g^n\}_{n \in \mathbb{N}}$ pro libovolný prvek $g \in G$.

Každý prvek posloupnosti je prvkem G (uzavřenost vůči 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 $n \leq |G|$.

Generátory a rank grupy

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 ($\text{Rank}(G)$).

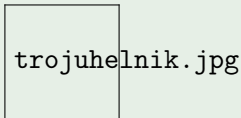
Example

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

Example

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 $\text{Rank}(D_6) = 2$.



Obrázek: Zobrazení grupy D_6 .

Example

Dihedrální 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 $r^n = e$, $s^2 = e$, $rs = sr^{-1}$.

Example

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.

Example

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 $|S_n| = n!$.

Example

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

Homomorfismus a isomorfismus grup

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: $\text{Ker } \varphi = \{x \in G \mid \varphi(x) = e_H\}$.

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

Example

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

Example

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

Example

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. $\varphi \in \text{Aut } G$.

Theorem

Všechny automorfismy grupy G tvoří grupu $\text{Aut } G$

Důkaz.

Identické zobrazení - jednotka v $\text{Aut } G$, protože $\varphi \in \text{Aut } G$ je bijekce, existuje φ^{-1} a $\phi \cdot \varphi = \psi$ leží v $\text{Aut } G$.



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 $(\forall x \in H)(|\varphi(x)| = |x|)$.

-
-

Podgrupy - proč ?

Pro studium vlastností a struktur grup je potřeba je rozdělit na "nedělitelné" grupy a podívat se jakým způsobem jsou z nich tyto grupy složeny.

Je to vlastně komplikovaná analogie rozkladu čísla na prvočinitele. Těmito prvočiniteli jsou grupy speciálního typu.

(Matematikům to trvalo 100 let, než v roce 1980 našli všechny tyto grupy)

A způsoby jejich skládání do složitějších celků se řeší dodnes.

*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 vůči jejich inverzi.)*

Example

- Množina $\{E, A\}$ je podgrupou v D_6 ($A^2 = E$, $A^{-1} = A$).
- Rotace kolem pevné osy je podgrupou v $SU(2)$
- Komplexní čísla jsou podgrupou v kvaternionech
- jakákoliv permutace generuje podgrupu v symetrické grupě

Věta pro zjednodušení důkazu podgrup

Theorem

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

Důkaz.

Implikace $\Rightarrow$ plyne přímo z definice podgrupy.

Dokážeme opačnou implikaci $\Leftarrow$, tj. že H je grupa.

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 . □

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

Důležité podgrupy - centralizátory

Bud' $\emptyset \neq A \subset G$ libovolná podmnožina.

Definujeme **centralizátor** množiny A v G jako: $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ pro } \forall a \in A\}$.

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

Nebo se dá říct, že jsou to všechny prvky $g \in G$, které po působení na každý prvek z A "akcí" $(gag^{-1} = a)$ ponechá tento prvek na místě.

Theorem

Množina $C_G(A)$ je podgrupa v G .

Důkaz.

*Víme, že $C_G(A)$ je neprázdná, $e \in C_G(A)$ ($eae^{-1} = a$).
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.



Definujeme

centrum grupy G je množina $Z(G) = \{g \in G \mid gfg^{-1} = f \text{ pro } \forall f \in G\}$.

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

Centrum je centralizátor celé grupy

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

*Bud' $\emptyset \neq A \subset G$. Definujeme **normalizátor** A v G jako: $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.*

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 $C_G(A)$. Tady je opět A libovolná množina. Později zavedeme

normální podgrupu, kterých může být v grupě mnoho. Jsou to takové **podgrupy**, které normalizuje celá grupa.

Corollary

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

Důkaz.

$N_G(A) \leq G$: Použijeme značení z předchozího.

- 1 $N_G(A) \neq \emptyset$, protože $e \in N_G(A)$.
- 2 Nechť $x, y \in N_G(A)$, 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 Nechť $x \in N_G(A)$. 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. □

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

U končných grup je jednotkový prvek vždy nějakou nenulovou mocninou generátoru.

Cyklická grupa má $\text{rank}=1$. Může být generována i různými prvky -např. $\mathbb{Z}_p$

Cyklická grupa je vždy abelovská (komutativní).

Theorem

Dvě cyklické grupy $\langle x \rangle$ a $\langle \xi \rangle$ stejného řádu jsou isomorfní.

Důkaz.

Pro konečné grupy máme izomorfismus: $\varphi(x) = \xi, \varphi(x^n) = \xi^n$

Pro nekonečnou grupu $\langle x \rangle$: $\varphi : G \rightarrow \mathbb{Z}$

$$\varphi(e) = 0, \varphi(x) = 1, \varphi(x^n) = n, n \in \mathbb{N},$$



Theorem

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

Důkaz.

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



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

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

- 1) Pokud $x^n = 1$ a $x^m = 1$, ($m, n \in \mathbb{Z} \setminus \{0\}$), potom $x^d = 1$, kde $d = \gcd(m, n)$
- 2) Navíc pokud $x^m = 1$, pak $|x|$ dělí m .

Důkaz:

1)

$d = mr + ns$ - Euclidův algoritmus

$$x^d = x^{mr+ns} = x^{mr} x^{ns} = 1$$

2)

$x^m = 1$, necht' $|x| = n$. Pak necht' $d = \gcd(m, n)$ a $x^d = 1$, d je menší rovno než n , n je řád -nejmenší takové číslo $\Rightarrow d = n$ a $d|m$. Symbol $|$ znamená první číslo dělí druhé

Theorem

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 $\alpha \in \mathbb{Z} \setminus \{0\}$.

Důkaz.

1) Sporem

$|G| = \infty$ znamená, že $|x| = \infty$. Nechť $(\exists n \in \mathbb{N})$ tak, že $|x^\alpha| = n$, tj. $((x^\alpha)^n = x^{n\alpha} = e)$ - spor. Dále nechť $x^\alpha = x^\beta$. Potom $x^{\alpha-\beta} = x^0 = 1$ (tedy $|x| = \alpha - \beta$), což je též spor. □

Pokud je $n\alpha$ záporné, $-n\alpha$ je kladné číslo - řád prvku.

Důkaz.

2) Víme tedy, že $|x| = n$. Označme si $d = \gcd(n, \alpha)$. Musí existovat celá čísla c a d taková, že $\alpha = cd$ a $n = bd$, $\gcd(b, c) = 1$. Platí:

$$(x^\alpha)^b = x^{\alpha b} = x^{d c b} = x^{n c} = e.$$

Nyní ukážeme sporem, že $b \in \mathbb{N}$ je nejmenší takové číslo: Nechť $|x^\alpha| \mid b$ (dělí b). Potom

$$\exists k < b, x^{\alpha k} = e, n \mid \alpha k, db \mid dck, b \mid ck.$$

Ale protože $\gcd(b, c) = 1$, b musí dělit k a to je spor.
(Doporučuji si to vyzkoušet na konkrétních číslech, třeba $n = 4$ a $\alpha = 6$.)



Theorem

Nechť $H = \langle x \rangle$, potom

- ① $|x| = \infty \Rightarrow \{H = \langle x^\alpha \rangle \Leftrightarrow \alpha = \pm 1\}$
- ② $|x| = n < \infty \Rightarrow \{H = \langle x^\alpha \rangle \Leftrightarrow \gcd(\alpha, n) = 1\}$
- ③ *Každá podgrupa grupy $\langle x \rangle$ je cyklická.*

Podgrupy generované podmnožinou grupy

Máme-li nějakou podmnožinu M prvků z grupy, potom můžeme definovat podgrupu generovanou touto podmnožinou - pozor pro nekomutativní grupy. Je to minimální podgrupa, který obsahuje všechny prvky z M . Snadno se ukáže, že průnik podgrup je opět podgrupa - např. napřed pro dvě a potom indukcí.

$$K = G \cap H.$$

Pro $\forall x, y \in K$ platí $xy^{-1} \in K$. Vše leží v G i H .

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

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

Pro konečný počet prvků $A = \{a_1, a_2, \dots, a_k\}$ píšeme:

$$\langle A \rangle = \langle a_1, a_2, \dots, a_k \rangle .$$

Nechť $\overline{A} = \{a_{i_1}^{\epsilon_{i_1}} a_{i_2}^{\epsilon_{i_2}} a_{i_3}^{\epsilon_{i_3}} a_{i_4}^{\epsilon_{i_4}} \dots, \epsilon_{i_1} = \pm 1, k \in \mathbb{N} \cup \{0\}\}$ a $\overline{A} = 1$ pro $A = \emptyset$,
potom

$$\overline{A} = \langle A \rangle, \quad A \subseteq G.$$

Grafy grup - svazy podgrup

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

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

- ❶ *reflexivita:* $(\forall x \in M)(x \preceq x)$,
- ❷ *tranzitivita:* $(\forall x, y, z \in M)(x \preceq y \wedge y \preceq z \rightarrow x \preceq z)$,
- ❸ *slabá antisymetrie:* $(\forall x, y \in M)(x \preceq y \wedge y \preceq x \rightarrow x = y)$.

Example

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

Example

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

usporadani.jpg

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

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

- **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 .

Svaz a modulární svaz

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

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

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

Definice:

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

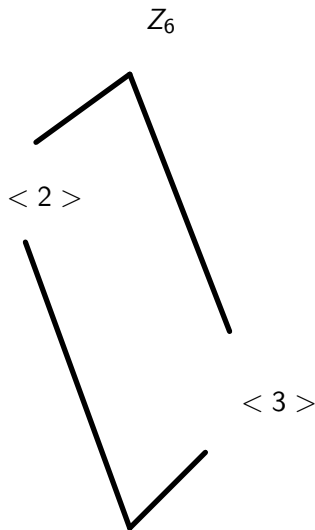
Example

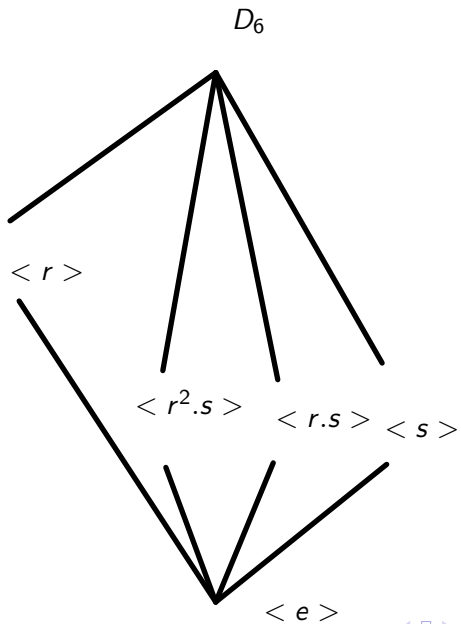
Nechť je relace uspořádání $a \preceq b$ vlastnost, že a dělí b , potom $\{4, 6, 8\}$ není svaz - $\sup = 24$, $\inf = 2$. Zatímco $\{2, 4, 6, 8, 24\}$ s daným uspořádáním svaz je.

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

Konstrukce **Hasseova diagramu** konečné grupy G přes podgrupy:

- Najdeme všechny podgrupy G a seřadíme je podle jejich řádu. Grupu G umístíme nejvýše a grupu 1 nejnižše. 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.)
- Mezi každými dvěma podgrupami $A \leq B$ existuje spojnice, ale může vést přes celý řetězec podgrup a těchto spojníc může být i více. Příklad je na obrázku.



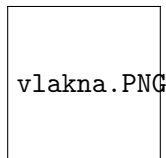
D_6 

Konstrukce Hasseova diagramu podgrup konečné grupy G :

Remark

Najdeme všechny podgrupy G a seřadíme je podle jejich řádu. Grupu G umístíme nejvýše a grupu 1 nejnižše. 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.)

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



Obrázek: Znáznornění vláken homomorfismu. Převzato z Dummit,Foote

Homomorfismus $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_5$

Example

-5	-4	-3	-2	-1	$\mathbb{Z}$
0	1	2	3	4	
5	6	7	8	9	
...	...	...	...	...	
± 15	1 ± 15	2 ± 15	3 ± 15	4 ± 15	
...	...	...	...	...	$\mathbb{Z}_5$
$\pm n5$	$1 \pm n5$	$2 \pm n5$	$3 \pm n5$	$4 \pm n5$	
0	1	2	3	4	

Vlákno jsou složené z prvků v sloupci, vlákno jsou všechny prvky ve sloupci.

Definice:

Jádro homomorfismu $\varphi : G \rightarrow H$ jsou všechny prvky G , které se zobrazí na e_H .

$$\text{Ker } \varphi \equiv \{g \in G \mid \varphi(g) = e_H\}$$

Corollary

Pro homomorfismus $\varphi : G \rightarrow H$ platí:

- ❶ $\varphi(e_G) = e_H$
- ❷ $\varphi(g^{-1}) = \varphi(g)^{-1}$ *pro* $\forall g \in G$
- ❸ $\varphi(g^n) = \varphi(g)^n$ *pro* $\forall n \in \mathbb{Z}$
- ❹ $\text{Ker } \varphi \leq G$
- ❺ $\varphi(G) \leq H$

Důkaz.

- ① $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) \implies$ (krácení v H) $\varphi(e_G) = e_H$.
- ② $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H$, 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 $h_1 = \varphi(g_1)$.



Rozklad do tříd ekvivalence: $a, b \in G, a \sim b \Leftrightarrow \exists k \in K, ka = b$

Mějme homomorfismus $\varphi : G \rightarrow H$ s jádrem $\text{Ker } \varphi = K$. Potom **faktor grupa** G/K (G modulo K) je grupa, jejíž prvky tvoří vlákna homomorfismu φ a operace násobení mezi vlákny je definovaná pomocí násobení mezi příslušnými obrazy homomorfismu v grupě H .

pokud X je vlákno nad a a Y je vlákno nad b , pak prvek $XY \in G/K$ je vlákno nad ab .

Navíc jednotkovým prvkem ve faktor grupě je jádro homomorfismu - podgrupa K .

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

Theorem

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 $X_a \subset uK$ 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 $g \in uK$.



Levé a pravé třídy

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.)

*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**.*

Že to neplatí obecně: D_6 , $K \equiv \{E, A\}$ a máme vevou a pravou třídu $BK = \{B, D\}$, ale $KB = \{B, F\}$

Theorem

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

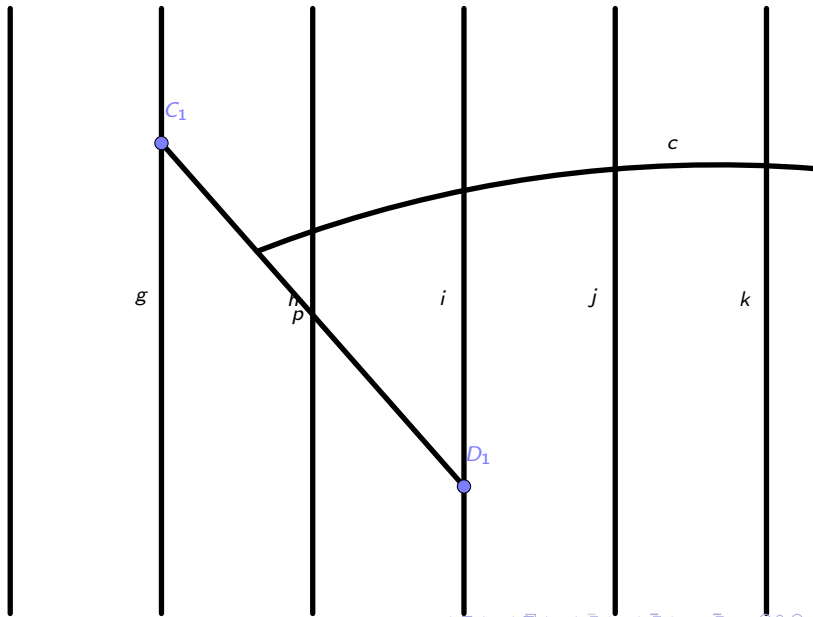
Důkaz.

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 32 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 $Z = uvK$.





Theorem

Nechť $N \leq G$, 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.

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 $uN = vN$. Vezměme $x \in uN \cap vN$, 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.

Dobře definovaná operace

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.

Definice

Operace $\circ$ na levých třídách N v G je **dobře definovaná**, když $\forall u, v \in G$ platí

$$u, u_1 \in uN, \quad v, v_1 \in vN \Rightarrow (uv)N = (u_1v_1)N = uN \circ vN$$

Theorem

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

- 1 Operace na levých třídách definovaná jako $uN \circ vN = (uv)N$ 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 s touto operací grupou, jednotkovým prvkem eN a inverzními prvky $(gN)^{-1} = g^{-1}N$.*

Důkaz 1

($\Rightarrow$) Nechť je operace na levých třídách dobře definovaná, tedy

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

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

$$g^{-1}N = ng^{-1}N$$

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 $gng^{-1} = n_1 \in N$.

($\Leftarrow$) 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 $u_1v_1 \in uvN$:

$$u_1v_1 = (un)(vm) = u(vv^{-1})nv m = (uv)(v^{-1}nv)m = (uv)(n_1)m = uv n_2$$

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 $uvN = u_1v_1N$.

Je-li operace na levých třídách dobře definovaná, axiomy grupy se přenášejí z G . Pro $\forall u, v, w \in G$

Asociativita:

$$(uN) \circ (vN \circ wN) = uN \circ (vwN) = u(vw)N = (uv)wN = (uN \circ vN) \circ (wN).$$

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

A tudíž jsem schopen vytvořit faktor grupu na levých třídách.

Definice:

Normální podgrupou H v G nazvenme každou podgrupu, kterou normalizuje celá grupa, značíme $H \trianglelefteq G$, tj.

$$H \trianglelefteq G \Leftrightarrow N_G(H).$$

Vlatnost $\trianglelefteq$ není tranzitivní, zatímco $\leq$ je tranzitivní.

Definice:

- 1 Prvek $m = gng^{-1}$ se nazývá **konjugovaný** k n prvkem g .
- 2 Bud' $A \subset G$ libovolná podmnožina grupy. Množina $M = gAg^{-1}$ se nazývá **konjugovaná** k A prvkem g .

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.

Theorem

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 přímo z definice.

Theorem

Nechť $N \leq G$, potom $N \trianglelefteq G$ právě tehdy když $\exists$ homomorfismus $\varphi(G)$ takový, že $N = \text{Ker } \varphi$.

Důkaz.

- ($\Leftarrow$) Podle jedné z předchozích vět víme, že levé a pravé třídy dle jádra homomorfismu jsou stejné ($gN = Ng$), což je podle věty ekvivalentní normálnosti grupy.
- ($\Rightarrow$) Nyní máme $N \trianglelefteq G$ a označíme $H = G/N$. Operace na levých třídách pro normální grupu je 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: $\text{Ker } (\pi) = \{g \in G \mid \pi(g) = eN\} = \{g \in G \mid gN = eN\} = \{g \in G \mid g \in N\} = N$.



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

Definice:

*Bud' $N \trianglelefteq G$, pak zobrazení $\pi : G \rightarrow G/N : \pi(g) = gN$ nazýváme **přírozená projekce** G na G/N .*

Shrnutí:

Homomorfismus $\rightarrow$ jádro $\rightarrow$ faktor grupa $\rightarrow$ dobře definovaná operace $\rightarrow$ normální podgrupa $\rightarrow$ přírozená projekce (homomorfismus)

Theorem

Nechť $N \trianglelefteq G$. Množina levých tříd G dle N tvoří rozklad G dle N ,

$$G = N \cup a_1 N \cup a_2 N \cup a_3 N \cup \dots$$

a platí:

$$\forall u, v \in G \text{ je } uN = vN \Leftrightarrow v^{-1}u \in N.$$

Důkaz.

$$(\Leftarrow) uk = vk' \Leftarrow v^{-1}u = k'k^{-1} \in N$$

$$(\Rightarrow) \text{Nechť } k = v^{-1}u \in N, \text{ tj.}$$

$$N = kN = (v^{-1}u)N = v^{-1}N \circ uN \Rightarrow (vN)^{-1} \circ uN = N, \Rightarrow vN = uN$$



Theorem (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 $k = \frac{|G|}{n}$.



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

Důsledky:

- Grupa G prvočíselného řádu nemůže mít netriviální normální podgrupu. Tato grupa je cyklická a $G \simeq \mathbb{Z}_p$

Důkaz:

$e \neq x \in G$, a navíc $|\langle x \rangle| > 1$. $|\langle x \rangle|$ dělí $|G|$. Ale $|G|$ je prvočíslo, proto $|x| = p$.



$$x^{|G|} = e$$

Z Lagrangeovy věty $|G|$ je násobek $|x|$, $\frac{|G|}{|x|} = m$ tj. $x^{|x|m} = e = x^{|G|}$

- !! Obráceně neplatí: pokud m dělí $|G|$, potom nemusí existovat podgrupa řádu m !! (A_4 nemá podgrupu řádu 6)

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

Pro konečné grupy platí

$$|G : H| = \frac{|G|}{|H|}.$$

Důsledek:

Podgrupa s indexem 2 je normální.

$$\forall g \in G, \quad gG = G = H \cup gH, \quad g \notin H, \quad Gg = G = H \cup Hg \Rightarrow gH = Hg$$

Remark

Remark

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 $gH = Hg$.

Remark

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

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

Důkaz.

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

Grupa prvočíselného řádu je cyklická.

Theorem (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 . □

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

Remark

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.)

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

Theorem

Nechť H a K jsou podgrupy konečné grupy G , pak

$$|HK| = \frac{|H||K|}{|H \cap K|}. \quad (1)$$

Důkaz.

HK můžeme napsat jako sjednocení levých tříd K ,

$$HK = \bigcup_{h \in H} hK. \quad (2)$$

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

$$h_1K = h_2K \Leftrightarrow h_2^{-1}h_1 \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K). \quad (3)$$

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

Theorem

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

Důkaz.

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

$$ab^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = h_1 k_3 h_2^{-1} \quad (4)$$

kde $k_3 = k_1 k_2^{-1} \in K$. Užitím předpokladu můžeme napsat $k_3 h_2^{-1} = h_4 k_4$ a dostáváme

$$ab^{-1} = (h_1 h_4) k_4 \in HK. \quad (5)$$

-) *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 $a = h_1 k_1$ pro nějaké $h_1 \in H, k_1 \in K$. Dostáváme tedy*

$$hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH. \quad (6)$$

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 $H \leq G$.

Důkaz.

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

$$hk = (hkh^{-1})h \in KH. \quad (7)$$

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

Theorem (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 32 a ?? . 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. □

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

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

Theorem (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 12 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 $\varphi(a) = aB$:

$$\varphi(a_1 a_2) = (a_1 a_2)B = a_1 B a_2 B = \varphi(a_1) \varphi(a_2). \quad (8)$$

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 $A/A \cap B \cong AB/B$. □

Theorem (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 faktor grupu 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. Přímým výpočtem za využití normality podgrup ověříme platnost $K/H \trianglelefteq G/H$:

$$\begin{aligned} gHkH(gH)^{-1} &= gH(g^{-1}g)k(g^{-1}g)Hg^{-1}H = (gHg^{-1})(gkg^{-1})(gHg^{-1})H = \\ &= Hk_1H = (k_1k_1^{-1})Hk_1H = k_1H \in K/H. \end{aligned} \quad (9)$$

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

$$\text{Ker } \varphi = \{gH \in G/H \mid \varphi(gH) = K\} = \{gH \in G/H \mid gK = K\} = \{gH \in G/H \mid g \in K\} = K/H \quad (10)$$

Remark

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 .

Theorem

[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 podgroupu A/N ze druhé. Zobrazení θ má navíc tyto vlastnosti: Pro $A, B \leq G$ obsahující N jako podgroupu 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. Necht' $A/N = B/N$. 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

Theorem

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 39 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.



Grupa G (konečná i nekonečná) se nazývá **jednoduchá**, pokud $|G| > 1$ a

jejími jedinými normálními podgrupami jsou e a G .

V grupě G řadu 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 .

Theorem (Jordan-Hölder)

Bud' $G \neq e$ konečná grupa. Pak:

- ❶ *G má kompoziční řadu,*
- ❷ *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*

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1} \quad 1 \leq i \leq r. \quad (11)$$

Důkaz J–H první část.

Mějme nejdelší možný řetěz normálních 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 69 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

Pro důkaz druhé části nejprve vyslovíme a dokážeme následující lemma:

Lemma

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 $N/(M \cap N) \cong G/M$.

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 $NM/M = G/M$ a $MN = G$. Potom závěry $M/(M \cap N) \cong G/N$ a $N/(M \cap N) \cong G/M$ plynou z 2. VOI 67. $\square$

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 67), 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 $N/(M \cap N) \cong (N \cap M)/(M \cap N) \cong M/M$, takže permutační vlastnost faktorgrup

Theorem

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.



Theorem (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...



Akce grupy na množině

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 $(\forall a \in A)(e \cdot a = a).$

Theorem

Bud' 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

$(\varphi(f) \circ \varphi(g))(a) = \sigma_f(\sigma_g(a)) = f \cdot (g \cdot a) = (fg) \cdot a = \sigma_{fg}(a) = \varphi(fg)(a).$



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

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.

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

Theorem

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 . $\square$

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

Corollary

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

$$\text{Ker}(\cdot) = \bigcap_{a \in A} G_a. \quad (12)$$

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

Theorem

Bud' $H \leq G$, akce G působí na levých třídách $\{g_iH\}_i = A$ 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. $g \in xHx^{-1}$. □

Theorem (Cayley)

Každá grupa je isomorfní 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

$$\Phi(g_1g_2)x = (g_1g_2)x = g_1(\Phi(g_2)x) = \Phi(g_1)\Phi(g_2)x.$$

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

$$\Phi(g_1) = \Phi(g_2) \Leftrightarrow \varphi_{g_1} = \varphi_{g_2} \Leftrightarrow (\text{aplikace na } x) \ g_1x = g_2x \Leftrightarrow g_1 = g_2.$$

Máme tudíž $G \cong \Im\Phi$, což je podle předešlého tvrzení podgrupa S_G . □

Buď 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 88) 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 $|G/K|/|G/H| = |K/H|$, z čehož plyne $p = |G/K| = |G/H||K/H| = p|K/H|$. Rovnost $|K/H| = 1$ však znamená $H = K$, což je normální podgrupa G . □

Remark

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 $g \in G$.

Remark

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

Theorem

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

- 1 Relace na A definovaná přes akci G jako $a \sim ba = g \cdot b$ 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 $g \cdot a = h \cdot ah^{-1}g \in G_a g G_a = h G_a$ je taky prosté.



Remark

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

Remark

Dále budeme pod pojmem orbita rozumět příslušnou třídu ekvivalence konjugace.

Theorem (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

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

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 $|P| = |Z(P)| + \sum_{i=1}^r |P : C_G(g_i)|$ plyne, že $|Z(P)|$ je dělitelné p , protože $|P|$ je dělitelné p z předpokladu a $|P : C_G(g_i)|$ je dělitelné p z předpokladu a Lagrangeovy věty. ($C_G(g_i)$ 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. □

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

Důkaz.

$Z(P) \trianglelefteq P$. 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 : Nechť $|P/Z(P)| = p$, 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. □

Sylowova věta

Buďte 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 $\text{Syl}_p(G)$ a počet těchto podgrup $n_p(G)$ (nebo jen n_p , je-li grupa jasná z kontextu).

Lemma

Nechť $P \in \text{Syl}_p(G)$ 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 $H \leq P$.



Theorem (Sylow)

Bud' G grupa řádu $p^\alpha m$, kde p je prvočíslo a $p \nmid m$. Pak:

- 1 *Existuje Sylowova p -podgrupa, tedy $\text{Syl}_p(G) \neq \emptyset$.*
- 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. Necht' tedy existuje Sylowova p -podgrupa pro všechny grupy menšího řádu než $|G|$.
Když $p \mid |Z(G)|$, pak podle věty 70 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 $p \nmid |Z(G)|$.
Necht' $g_1, g_2, \dots, g_r$ jsou reprezentanti různých tříd neobsažených v*

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

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



Theorem (Cauchy)

Necht' 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 . □

Definice:

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

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.)

„Součin“ podgrup $K, H \leq G$ je množina $KH = \{kh | k \in K, h \in H\}$.

!! Součin podgrup nemusí být podgrupou!!

Theorem

Necht' H a K jsou podgrupy konečné grupy G , pak

$$|HK| = \frac{|H||K|}{|H \cap K|}. \quad (24)$$

Princip důkazu: Ukážeme, že počet tříd hK je stejný jako počet tříd $h(K \cap H)$, tj.

$$HK = K \cup h_1K \cup \dots \cup h_sK$$

$$H = (K \cap H) \cup h_1(K \cap H) \cup \dots \cup h_s(K \cap H)$$

Důkaz.

HK můžeme napsat jako sjednocení levých tříd K ,

$$HK = \bigcup_{h \in H} hK. \quad (25)$$

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

$$h_1K = h_2K \Leftrightarrow h_2^{-1}h_1 \in H \cap K \Leftrightarrow h_1(H \cap K) = h_2(H \cap K). \quad (26)$$

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. □

Theorem

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 $a = h_1 k_1$ a $b = h_2 k_2$ pro nějaké $h_1, h_2 \in H$ a $k_1, k_2 \in K$. Tedy

$$ab^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = h_1 k_3 h_2^{-1} \quad (27)$$

kde $k_3 = k_1 k_2^{-1} \in K$. Užitím předpokladu můžeme napsat $k_3 h_2^{-1} = h_4 k_4$ a dostáváme

$$ab^{-1} = (h_1 h_4) k_4 \in HK. \quad (28)$$



Důkaz.

($\Rightarrow$)

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

$$hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH. \quad (29)$$



Corollary

Necht' $H, K \leq G$ a $H \leq N_G(K)$, pak $HK \leq G$. Speciálně pokud $K \trianglelefteq G$, pak $HK \leq G$ pro libovolnou $H \leq G$.

Důkaz.

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

$$hk = (hkh^{-1})h \in KH. \quad (30)$$

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

1. Věta o isomorfismu

Theorem (1. VOI)

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

Důkaz.

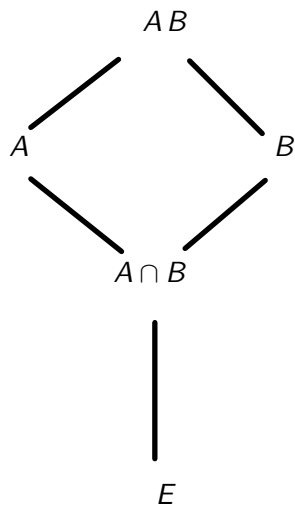
První část je zřejmá z předchozích vět. Důkaz druhé spočívá v ověření, že $\varphi' : G/\text{Ker } \varphi \rightarrow \varphi(G) : \varphi'(g\text{Ker } \varphi) = \varphi(g)$ je izomorfismus, což je plyne z definic a předchozího. □

Corollary

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

- ① φ je izomorfismus $\Leftrightarrow \text{Ker } \varphi = e_G$,*
- ② $|G/\text{Ker } \varphi| = |\varphi(G)|$.*

2. Věta o isomorfismu - diamantová



Theorem (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 $AB/B \cong A/A \cap B$.

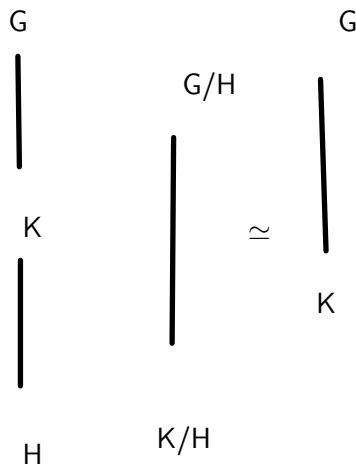
Důkaz.

Z důsledku 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 $\varphi(a) = aB$:

$$\varphi(a_1 a_2) = (a_1 a_2)B = a_1 B a_2 B = \varphi(a_1) \varphi(a_2). \quad (31)$$

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 $A/A \cap B \cong AB/B$. □

3. Věta o isomorfismu - o faktor grupách z faktor grup



Theorem (3. VOI)

Bud' G grupa a $H \trianglelefteq G$, $K \trianglelefteq G$ a $H \leq K$. Potom $K/H \trianglelefteq G/H$ a $(G/H)/(K/H) \cong \bar{G}/\bar{K}$. Označíme-li faktor grupu 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. Přímým výpočtem za využití normality podgrup ověříme platnost $K/H \trianglelefteq G/H$:

$$\begin{aligned} gHkH(gH)^{-1} &= gH(g^{-1}g)k(g^{-1}g)Hg^{-1}H = (gHg^{-1})(gkg^{-1})(gHg^{-1})H = \\ &= Hk_1H = (k_1k_1^{-1})Hk_1H = k_1H \in K/H. \end{aligned} \quad (32)$$

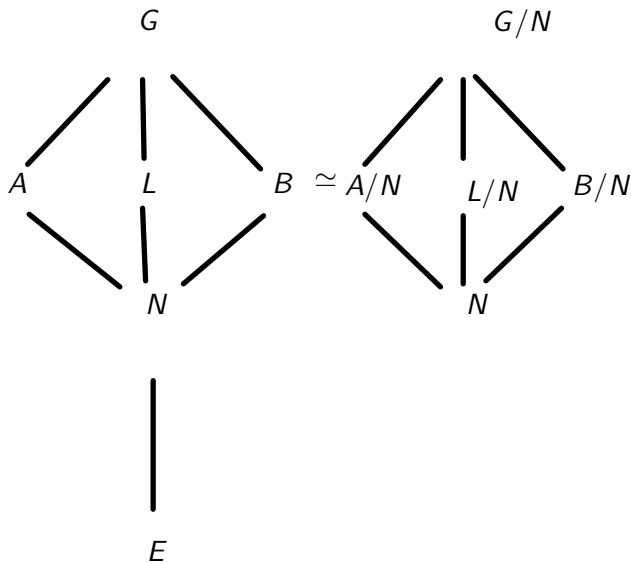
Definujeme homomorfismus $\varphi : G/H \rightarrow G/K$ předpisem $\varphi(gH) = gK$. Abychom ukázali že φ je dobře definované, vezmeme $g_1H = g_2H$. Potom $g_1 = g_2h$ pro nějaké $h \in H$. Protože $H \leq K$, je taky $h \in K$, proto $g_1K = g_2K$. Tudíž $\varphi(g_1H) = \varphi(g_2H)$ a φ je dobře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

$$\text{Ker } \varphi = \{gH \in G/H \mid \varphi(gH) = K\} = \{gH \in G/H \mid gK = K\} = \quad (33)$$

$$= \{gH \in G/H \mid g \in K\} = K/H, \quad (34)$$

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

4. Věta o isomorfismu - o grafech faktor grup



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 .

Theorem

[4. VOI, „mřížková“] Bud' G grupa a $N \trianglelefteq G$. Potom existuje bijekce θ z množiny W 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

- ❶ $B \leq A \Leftrightarrow B/N \leq A/N,$
- ❷ Je-li $A \leq B$, pak $|B : A| = |B/N : A/N|,$
- ❸ $\langle A, B \rangle / N = \langle A/N, B/N \rangle,$
- ❹ $A/N \cap B/N = (A \cap B)/N,$
- ❺ $A \trianglelefteq G \Leftrightarrow A/N \trianglelefteq G/N.$

Důkaz 1) a 2)

Ověříme, že zobrazení θ definované pomocí $A \mapsto A/N$ je bijekce: Nejprve prostota. Necht' $A/N = B/N$. 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 $\phi^{-1}(S) = \{s \in G \mid sN \in S\}$ je podgrupa G (platí $uNvN = uvN$) obsahující $N = \phi^{-1}(\{e\})$ a $\theta(\phi^{-1}(S)) = \{sN \mid sN \in S\} = S$, 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.

Důkaz 3) a 5)

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 .

Theorem

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 39 G cyklická a tedy generovaná nějakým prvkem řádu $|G|$. Dále tedy předpokládáme $|G| > p$.

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.



Prostá grupa a kompoziční řady

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

V grupě G řadu 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 .

Theorem (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

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1} \quad 1 \leq i \leq r. \quad (35)$$

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 69 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. □

Pro důkaz druhé části nejprve vyslovíme a dokážeme následující lemma:

Lemma

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 $N/(M \cap N) \cong G/M$.

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 67. $\square$

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), proto rozšířením kompozitní řady pro K získáme kompozitní řady pro M a N , konkrétně

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



Důkaz.

Díky indukčnímu předpokladu platí $r - 1 = t + 1 = s - 1$ (stejně délky řetězců), tj. $r = s$, a také vlastnost vůči permutacím faktorgrup. Díky 2.VOI 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

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



Corollary

Každá konečná grupa má faktorizaci, tj. kompoziční řadu, která není obecně jednoznačná.

Theorem

Existuje 18 (nekonečných) rodin jednoduchých grup a 26 prostých grup, které nepatří do žádné z těchto skupin (sporadické prosté grupy) takových, že každá konečná prostá 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.



Theorem (Důsledek Feit–Thompsonovy věty)

Všechny prosté konečné grupy lichého řádu jsou abelovské, přesněji $|G| = 2n - 1 \Leftrightarrow 2n + 1 = p, G \cong \mathbb{Z}_p$.

Důkaz.

255 stran...



Akce grupy na množině

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 $(\forall a \in A)(e \cdot a = a)$.

Theorem

Bud' 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
 $(\varphi(f) \circ \varphi(g))(a) = \sigma_f(\sigma_g(a)) = f \cdot (g \cdot a) = (fg) \cdot a = \sigma_{fg}(a) = \varphi(fg)(a)$.



Pro každou grupu G a neprázdnou množinu A existuje bijekce mezi akcemi

G na množině A a homomorfismy G do symetrické grupy S_A .

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.

Mějme grupu G a její akci $\cdot : G \times S \rightarrow S$ na množinu S a necht' $s \in S$ je pevně zvolený prvek. Potom **stabilizátor** s v G je: $G_s = \{g \in G \mid g \cdot s = s\}$.

Orbita s v G je $O_s = \{g \cdot s \mid g \in G\}$, občas značeno též $G \cdot s$.

Theorem

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 . □

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

Corollary

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

$$\text{Ker}(\cdot) = \bigcap_{a \in A} G_a. \quad (36)$$

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

Theorem

Bud' $H \leq G$, akce G působí na levých třídách $\{g_iH\}_i = A$ 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. $g \in xHx^{-1}$. □

Theorem (Cayley)

Každá grupa je isomorfní 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

$$\Phi(g_1g_2)x = (g_1g_2)x = g_1(\Phi(g_2)x) = \Phi(g_1)\Phi(g_2)x.$$

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

$$\Phi(g_1) = \Phi(g_2) \Leftrightarrow \varphi_{g_1} = \varphi_{g_2} \Leftrightarrow (\text{aplikace na } x) \ g_1x = g_2x \Leftrightarrow g_1 = g_2.$$

Máme tudíž $G \cong \Im\Phi$, což je podle předešlého tvrzení podgrupa S_G . □

Buď 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 88) 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 $|G/K|/|G/H| = |K/H|$, z čehož plyne $p = |G/K| = |G/H||K/H| = p|K/H|$. Rovnost $|K/H| = 1$ však znamená $H = K$, což je normální podgrupa G . □

Remark

Bud'te 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 $g \in G$.

Remark

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

Theorem

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

- 1 Relace na A definovaná přes akci G jako $a \sim ba = g \cdot b$ 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 $g \cdot a = h \cdot ah^{-1}g \in G_a g G_a = h G_a$ je taky prosté.



Remark

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

Remark

Dále budeme pod pojmem orbita rozumět příslušnou třídu ekvivalence konjugace.

Theorem (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

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

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 $|P| = |Z(P)| + \sum_{i=1}^r |P : C_G(g_i)|$ plyne, že $|Z(P)|$ je dělitelné p , protože $|P|$ je dělitelné p z předpokladu a $|P : C_G(g_i)|$ je dělitelné p z předpokladu a Lagrangeovy věty. ($C_G(g_i)$ 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. □

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

Důkaz.

$Z(P) \trianglelefteq P$. 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 : Nechť $|P/Z(P)| = p$, 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. □

Sylowova věta

Buďte 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

Nechť $P \in \text{Syl}_p(G)$ 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 $H \leq P$.



Theorem (Sylow)

Bud' G grupa řádu $p^\alpha m$, kde p je prvočíslo a $p \nmid m$. Pak:

- 1 *Existuje Sylowova p -podgrupa, tedy $\text{Syl}_p(G) \neq \emptyset$.*
- 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 $n_p \mid m$.*

Důkaz.

- 1 *Důkaz provedeme úplnou indukcí na $|G|$, přičemž pro $|G| = 1$ není co dokazovat. Necht' tedy existuje Sylowova p -podgrupa pro všechny grupy menšího řádu než $|G|$.
Když $p \mid |Z(G)|$, pak podle věty 70 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 $p \nmid |Z(G)|$.
Necht' $g_1, g_2, \dots, g_r$ jsou reprezentanti různých tříd neobsažených v*

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

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



- 1 Klasifikujte všechny konečné prosté grupy
trvalo 100 let do r. 1980
až 10 tisíc stran matematického textu
- 2 Najděte způsob vytváření grup z grup prostých.
Není úplně vyřešeno doposud. Např. má-li grupa všechny kompoziční faktory řádu 2 pak $|G| = 2^n$

Součástí procesu byla i **Feit – Thompsonova věta**

Výsledek 1

Theorem

Existuje 18 (nekonečných) rodin prostých grup a 26 sporadických prostých grup, které nepatří do žádné z těchto skupin. Každá konečná prostá grupa je izomorfní s některou z výše uvedených.

Důkaz.

Výsledek cca 100 let práce mnoha matematiků na 5000-10000 stránkách odborných časopisů.



Theorem

Každá prostá grupa lichého řádu je izomorfní $\mathbb{Z}_p$

Důkaz.

Důkaz byl publikován v r 1963 a byl na 255 stranách matematických výpočtů.



Corollary (Důsledek Feit–Thompsonovy věty)

Všechny prosté konečné grupy lichého řádu jsou abelovské, přesněji
 $|G| = 2n + 1 \Leftrightarrow 2n + 1 = p, G \cong \mathbb{Z}_p.$

Příklady:

- 1 $\mathbb{Z}_p$ pro všechna prvočísla
- 2 Alternující grupy A_n pro $n \geq 5$ (sudé permutace) A_5 je nejmenší prostá nekomutující grupa řádu 60. A_n je jádro homomorfismu $S_n \rightarrow \{-1, 1\}$
- 3 $SL_n(\mathbb{F})/Z(SL_n(\mathbb{F}))$, kromě $SL_2(\mathbb{F}_2)$ a $SL_2(\mathbb{F}_3)$, $\mathbb{F}$ je konečné těleso
- 4 Nejmenší sporadická grupa: Mathieu (1861●) M_{11} řádu 7920, založena na permutaci 11 prvků.
- 5 Další sporadická grupa: Mathieu M_{12} řádu 95040, založena na permutaci 12 prvků.
- 6 Největší sporadická grupa Monster - řád $\sim 8 \cdot 10^{53}$

Akce grupy na množině

Pro analýzu grup použijeme také akci grupy.

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 $(\forall a \in A)(e \cdot a = a).$

Theorem

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 $\varphi : G \rightarrow S_A$ (grupy do permutace množiny A) definované $\varphi(g) = \sigma_g$ je homomorfismus.

Důkaz.

1) Platí triviálně

2) Dokážeme, žeb je to homomorfismus: 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 $(\sigma_g \circ \sigma_{g^{-1}})(a) = a$.

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

$$(\varphi(f) \circ \varphi(g))(a) = \sigma_f(\sigma_g(a)) = f \cdot (g \cdot a) = (fg) \cdot a = \sigma_{fg}(a) = \varphi(fg)(a).$$



Corollary

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

Corollary

2) 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.

Označíme-li jednotlivé prvky např. pořadím, potom výsledek akce každého prvku z G bude matice s jednou jednotkou v každém řádku a každém sloupci – dostávám permutační reprezentci grupy.

Definice:

- 1 Pokud $G \rightarrow S_A$ je injektivní, nazýváme reprezentaci **věrnou**.
- 2 Každý homomorfismus $G \rightarrow S_A$, $A \neq \emptyset$ nazveme permutační reprezentací.

Tj. při věrné reprezentaci neztrácíme žádnou informaci o struktuře grupy. Jinak platí, že akce grupy G na A lze chápat jako věrnou reprezentaci faktor grupy $G/\text{Ker } \varphi$.

Zavedeme **levou regulární akci** grupy na sobě: $G \times G \rightarrow G$ jako $g : \mapsto ga$, a podobně **pravou regulární akci** grupy na sobě: $G \times G \rightarrow G$ jako $g : \mapsto ag$.

Mějme grupu G a její akci $\cdot : G \times A \rightarrow A$ na množině A , potom

- 1 Definujeme **jádro** akce jako: $\text{Ker}(\cdot) = \{g \in G \mid g \cdot s = s \text{ pro } \forall s \in S\}$.
- 2 Nechť $s \in A$ je pevně zvolený prvek. Potom **stabilizátor** s v G je:
 $G_s = \{g \in G \mid g \cdot s = s\}$.
- 3 Akce je věrná, pokud $\text{Ker } \varphi = e$.

Theorem

Platí $G_a \leq G$.

Důkaz.

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

Corollary

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

$$\text{Ker}(\cdot) = \bigcap_{a \in A} G_a. \quad (48)$$

Theorem (Rozklad grup díky akci)

Nechť grupa G působí akcí na množině A , potom:

- 1 Relace $\sim$ v A definovaná $a \sim b \Leftrightarrow \exists g \in G, a = g \cdot b$ je ekvivalence.
- 2 Pro každé $a \in A$ je počet prvků ve třídě ekvivalence roven indexu stabilizátoru $|G : G_a|$.

Důkaz.

- 1 $a = e \cdot a, a \sim a, a = g \cdot b, b = g^{-1}a, a = g \cdot b, b = h \cdot d, a = gh \cdot d$.
- 2 Třída ekvivalence $C_a = \{g \cdot a, \forall g \in G\}$, G_a stabilizátor a v G . Potom $b = g \cdot a = g \cdot (G_a \cdot a) = (gG_a) \cdot a$. G_a je podgrupou v G , rozložíme G do levých tříd

$$G = G_a \cup g_1 G_a \cup g_2 G_a \cup g_3 G_a \dots$$

a každé levé třídě odpovídá jeden prvek ve třídě ekvivalence. Těch je $|G : G_a|$.



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.

Orbita, tranzitivní akce

Nechť G působí na $A \neq \emptyset$ akcí, potom:

- 1 třída ekvivalence C_a se nazývá **orbita** G prvku a .
- 2 Akce G na A se nazývá **tranzitivní**, pokud existuje jenom jedna orbita.

Corollary

Zobrazení $C_a \rightarrow gG_a$ je bijekce.

Důkaz.

Na: pro $\forall g \in G, g \cdot a \in C_a$,

Prosté: $g \cdot a = h \cdot a \Leftrightarrow h^{-1}g \in G_a$, tj. $gG_a = hG_a$



Pokud $A = G$, tj. grupa působí akcí na sobě, každému $g \in G$ odpovídá permutace prvků grupy.

Akce je vždy tranzitivní a věrná. Stabilizátorem každého prvku je e .

Theorem

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

- ❶ *G působí tranzitivně na A ,*
- ❷ *stabilizátor eH v A je roven H ,*
- ❸ *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. $g \in xHx^{-1}, \forall x \in G$. □

Theorem (Cayley)

Každá grupa je isomorfní nějaké podgrupě grupy permutací. Je-li $|G| = n$, potom $\exists K \leq S_n$ tak, že $G \simeq K$

Důkaz.

Vezmeme v předchozí větě $H = e$, $\text{Ker } \pi_H = e$ a $G/e \simeq \pi_H(G) \leq S$. □

Corollary

Bud' p nejmenší prvočíslo dělící $|G|$ (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 p levých třídách H předpisem $x \cdot (gH) = xgH$. Tato akce indukuje homomorfismus G do S_p 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 prvočíslo dělící $|G|$, pak $|G/K| = p$. Díky 3.VOI platí $|G/K|/|G/H| = |K/H|$, z čehož plyne $p = |G/K| = |G/H||K/H| = p|K/H|$. Rovnost $|K/H| = 1$ však znamená $H = K$, což je normální podgrupa G . □

Konjugace je akce

Konjugace je zobrazení $G \times G \rightarrow G$, $g : a \mapsto gag^{-1}$ a je to akce G na G .

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

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

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

Dvě množiny S a T jsou konjugované, existuje - li $g \in G$ tak, že $T = gSg^{-1}$

Corollary

Počet konjugovaných podmnožin k podmnožině $S \subset G$ je index normalizátoru (= stabilizátoru) S , $|G : N_G(S)|$.

Důkaz.

Konjugace je akce, $N_G(S)$ je podgrupa, G lze rozložit do levých tříd atd. .



Theorem (rovnice tříd)

Nechť G je konečná grupa a $g_1, g_2, \dots, g_r$ reprezentanti konjugovaných tříd (různých orbit) neobsažených v centru $Z(G)$. 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 a konjugace je akce grupy na sobě, máme díky větě o počtu prvků v orbitě:

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

Corollary

Necht' 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 $|P| = |Z(P)| + \sum_{i=1}^r |P : C_G(g_i)|$ plyne, že $|Z(P)|$ je dělitelné p , protože $|P|$ je dělitelné p z předpokladu a $|P : C_G(g_i)|$ je dělitelné p z předpokladu a Lagrangeovy věty. ($C_G(g_i)$ 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. □

Corollary

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

Důkaz.

$Z(P) \trianglelefteq P$. 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 : Nechť $|P/Z(P)| = p$, 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 ale implikuje $P = Z(P)$, což je spor s předpokladem. Celkově tudíž $|P/Z(P)| = 1$ a $Z(P) = P$ je abelovská. □

Corollary

Dva prvky symetrické grupy jsou konjugované $\Leftrightarrow$ mají cykly stejného typu.

Důkaz.

$\sigma, \tau \in S_n$ a $\sigma = (a_1, a_2, a_3, \dots, a_k)(a_{k+1}, a_{k+1}, \dots)(\dots)$, tj. platí pro indexy $\sigma(i) = j$. Potom v indexech

$$\tau\sigma\tau^{-1} \tau(i) = \tau\sigma(i) = \tau(j)$$



Všechny automorfismy $G \rightarrow G$ tvoří grupu automorfismů $\text{Aut}(G)$.
 $\text{Aut}(G) \leq S_G$. Máme vnitřní a vnější automorfismy, tj. je to více než akce G na G .

Theorem

Nechť $H \trianglelefteq G$, akce G na H konjugací je automorfismus H pro každé jedno $g \in G$.

$$\varphi_g : h \mapsto ghg^{-1} \quad \psi : g \mapsto \varphi_g.$$

$$G/C_G(H) \simeq K \leq \text{Aut}(H)$$

Důkaz.

$$\text{Ker } \psi = \{g \in G \mid ghg^{-1} = h, \forall h \in H\} = C_G(H)$$

a 1.VOI



Definice:

Mějme grupu G , $g \in G$, definijeme **vnitřní automorfismus** gGg^{-1}
 $H \leq G$ je **charakteristická podgrupa**, pokud všechny automorfismy ji zobrazí na sebe. $\sigma \in \text{Aut}(G) \Rightarrow \sigma(H) = H$

Vlastnosti:

- 1 H je normální
- 2 je-li H jediná daného řádu, je charakteristická.

Definice: Bud'te 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 $\text{Syl}_p(G)$ a počet těchto podgrup $n_p(G)$ (nebo jen n_p , je-li grupa jasná z kontextu).

Lemma

Nechť $P \in \text{Syl}_p(G)$ 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 $H \leq P$.



Theorem (Sylow)

Bud' G grupa řádu $p^\alpha m$, kde p je prvočíslo a $p \nmid m$. Pak:

- ① Existuje Sylowova p -podgrupa, tedy $\text{Syl}_p(G) \neq \emptyset$.*
- 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 nějaké konjugované k P . Speciálně každé dvě Sylowovy p -podgrupy G jsou vzájemně konjugované 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 $n_p \mid m$.*

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 Cauchyho věty existuje $N \trianglelefteq Z(G)$ 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 $p \nmid |Z(G)|$.

$p \nmid |Z(G)|$

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

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|. \quad (49)$$

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

$$|G : C_G(g_i)| = \frac{p^\alpha m}{p^\alpha k}, \quad |H| = p^\alpha k, \quad \text{kde } p \nmid k, \quad (50)$$

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

Nechť Q je libovolná p -podgrupa G a necht'

$$\mathcal{S} = \{gPg^{-1} | g \in G\} \stackrel{\text{ozn.}}{=} \{P_1, P_2, \dots, P_r\} = \mathcal{S}. \quad (51)$$

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

$$\mathcal{S} = O_1 \cup O_2 \cup \dots \cup O_s \quad (52)$$

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 o počtu tříd ekvivalence 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

$$|O_i| = |Q : P_i \cap Q|, \quad 1 \leq i \leq s. \quad (53)$$

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

$$|O_1| = 1, \quad (54)$$

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

$$|O_i| = |P_1 : P_1 \cap P_i| > 1, \quad 2 \leq i \leq s. \quad (55)$$

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

$$p \mid |O_i|, \quad 2 \leq i \leq s. \quad (56)$$

Odtud

$$r = |O_1| + (|O_2| + \cdots + |O_s|) \equiv 1 \pmod p \quad (57)$$

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

$$|O_i| = |Q : Q \cap P_i| > 1, \quad 1 \leq i \leq s. \quad (58)$$

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 -podgrupu. Pak $Q \leq gPg^{-1}$ a zároveň $|gPg^{-1}| = |Q| = p^\alpha$, proto $gPg^{-1} = Q$.

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 počtu tříd ekvivalence a tomu, že všechny Sylowovy p -podgrupy jsou konjugované, dostáváme

$$n_p = |G : N_G(P)|, \quad \forall P \in \text{Syl}_p(G). \quad (59)$$

Corollary

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



Definice: Bud'te 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 $\text{Syl}_p(G)$ a počet těchto podgrup $n_p(G)$ (nebo jen n_p , je-li grupa jasná z kontextu).

Lemma

Nechť $P \in \text{Syl}_p(G)$ 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 $H \leq P$.



Theorem (Sylow)

Bud' G grupa řádu $p^\alpha m$, kde p je prvočíslo a $p \nmid m$. Pak:

- ① Existuje Sylowova p -podgrupa, tedy $\text{Syl}_p(G) \neq \emptyset$.*
- 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 nějaké konjugované k P . Speciálně každé dvě Sylowovy p -podgrupy G jsou vzájemně konjugované 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 $n_p \mid m$.*

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 Cauchyho věty existuje $N \trianglelefteq Z(G)$ 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 $p \nmid |Z(G)|$.

$p \nmid |Z(G)|$

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

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|. \quad (60)$$

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

$$|G : C_G(g_i)| = \frac{p^\alpha m}{p^\alpha k}, \quad |H| = p^\alpha k, \quad \text{kde } p \nmid k, \quad (61)$$

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

Nechť Q je libovolná p -podgrupa G a necht'

$$\mathcal{S} = \{gPg^{-1} | g \in G\} \stackrel{\text{ozn.}}{=} \{P_1, P_2, \dots, P_r\} = \mathcal{S}. \quad (62)$$

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

$$\mathcal{S} = O_1 \cup O_2 \cup \dots \cup O_s \quad (63)$$

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 o počtu tříd ekvivalence 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

$$|O_i| = |Q : P_i \cap Q|, \quad 1 \leq i \leq s. \quad (64)$$

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

$$|O_1| = 1, \quad (65)$$

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

$$|O_i| = |P_1 : P_1 \cap P_i| > 1, \quad 2 \leq i \leq s. \quad (66)$$

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

$$p \mid |O_i|, \quad 2 \leq i \leq s. \quad (67)$$

Odtud

$$r = |O_1| + (|O_2| + \cdots + |O_s|) \equiv 1 \pmod p \quad (68)$$

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

$$|O_i| = |Q : Q \cap P_i| > 1, \quad 1 \leq i \leq s. \quad (69)$$

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 -podgrupu. Pak $Q \leq gPg^{-1}$ a zároveň $|gPg^{-1}| = |Q| = p^\alpha$, proto $gPg^{-1} = Q$.

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 počtu tříd ekvivalence a tomu, že všechny Sylowovy p -podgrupy jsou konjugované, dostáváme

$$n_p = |G : N_G(P)|, \quad \forall P \in \text{Syl}_p(G). \quad (70)$$

Corollary

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

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



- $|G| < \infty$ a abelovská, pak má právě jednu Sylowovu p -podgroupu pro každé $p \mid |G|$.
- S_3 má 3 Syl_2 podgroupy ($\langle(1, 2)\rangle$, $\langle(2, 3)\rangle$, $\langle(1, 3)\rangle$) $n_2 = (1 + k2)$ a právě jednu Syl_3 $\langle(1, 2, 3)\rangle$ $n_3 = (1 + k3) - 4$ nedělí 3.
- S_4 má $n_2 = (1 + k2) = 1, 3, 5$ a $n_3 = (1 + k3) = 1, 4, 7$

Přímý součin grup

Jedná se o způsob konstrukce větších grup z menších.

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

- ❶ **Přímým součinem** konečné množiny grup $(G_1, *_1), (G_2, *_2), \dots (G_n, *_n)$ je grupa jejíž prvky je množina n -tic $(g_1, g_2, \dots, g_n), (h_1, h_2, \dots, h_n)$ ($g_i, h_j \in G_i$) s násobením definovaným po složkách.

$$(g_1, g_2, \dots, g_n) * (h_1, h_2, \dots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \dots, g_n *_n h_n). \quad (71)$$

Označení: $G = G_1 \times G_2 \times \dots \times G_n$

- ❷ **Přímým součinem** spočetné množiny grup $(G_1, *_1), (G_2, *_2), \dots (G_n, *_n)$ je grupa jejíž prvky je sočetná množina $(g_1, g_2, \dots), (h_1, h_2, \dots)$ ($g_i, h_j \in G_i$) s násobením definovaným po složkách.

$$(g_1, g_2, \dots) * (h_1, h_2, \dots) = (g_1 *_1 h_1, g_2 *_2 h_2, \dots). \quad (72)$$

Každá podgrupa $(1, 1, \dots, g_i, 1, 1, \dots)$ je normální. (Lze faktorizovat)
Je zřejmé, že výsledkem přímého součinu grup je opět grupa a to řádu $|G| = |G_1| |G_2| \dots |G_n|$ nebo nekonečného.

Klasifikace Abelovských grup

- 1 Grupa G je **konečně generovaná**, pokud existuje konečná množina $A \subset G$ taková, že $G = \langle A \rangle$.
- 2 Pro každé $r \in \mathbb{Z}$, $r \geq 0$, bud' $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ direktní součet r kopií grupy $\mathbb{Z}$, kde $\mathbb{Z}^0 = e$. Grupa $\mathbb{Z}^r$ se nazývá **volná Abelovská grupa řádu r** .

Theorem (základní věta Abelovských grup)

Bud' 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:
 - 1 $r \geq 0$ a $n_j \geq 2$ pro všechna j ,
 - 2 $n_{i+1} | n_i$ pro $1 \leq i \leq s-1$,
- 2 tento rozklad je jednoznačný.

Důkaz.

Bude zřejmé později.

$\Rightarrow$ Každý prvočíselný dělitel $|G|$ musí dělit n_1 .

Důsledek:

Je-li $n = p_1 p_2 p_3 \dots p_k$ součin k různých prvočísel, potom každá abelovská grupa řádu n je izomorfní Z_n

Example

Nechť $n = 180 = 2^2 \cdot 3^2 \cdot 5$, potom máme možnosti:

- ① $n_1 = 180$ – grupa Z_{180}
- ② $n_1 = 2^2 \cdot 3 \cdot 5$, $n_2 = 3$ – grupa $Z_{60} \times Z_3$
- ③ $n_1 = 2 \cdot 3^2 \cdot 5$, $n_2 = 2$ – grupa $Z_{90} \times Z_2$
- ④ $n_1 = 2 \cdot 3 \cdot 5$, $n_2 = 6$ – grupa $Z_{30} \times Z_6$

A toto jsou všechny možnosti neizomorfních abelovských grup řádu 180.

Věta se dá ekvivalentně napsat následujícím způsobem.

Rozklad abelovské grupy podle Sylowových podgrup

Podgrupy abelovské grupy jsou normální, každá Sylowova daného řádu je právě jedna .

Theorem

Bud' G abelovská grupa řádu $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, kde p_k jsou různá prvočísla. Potom

- ❶ $G \cong A_1 \times A_2 \times \dots \times A_k$, kde $|A_i| = p_i^{\alpha_i}$,
- ❷ pro každé $A_i \in A_1, A_2, \dots, A_k$, kde $|A_i| = p_i^{\alpha_i}$ je $A \simeq Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \dots \times Z_{p^{\beta_t}}$, 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)
- ❸ a rozklad v 1) a 2) je jednoznačný až na pořadí A_i .

Všimněte si, že $p_i^{\beta_{t+1}}$ dělí $p_i^{\beta_t}$.

Example

Nechť $n = 180 = 2^2 \cdot 3^2 \cdot 5$, potom máme dle této věty možnosti:

- ① $p^\beta = 2^2$, β má rozklad 2 nebo 1,1 a tomu odpovídají abelovské grupy $\mathbb{Z}_4$ a $\mathbb{Z}_2 \times \mathbb{Z}_2$
- ② $p^\beta = 3^2$, β má rozklad 2 nebo 1,1 a tomu odpovídají abelovské grupy $\mathbb{Z}_9$ a $\mathbb{Z}_3 \times \mathbb{Z}_3$
- ③ $p^\beta = 5^1$ β má rozklad 5 a tomu odpovídá abelovská grupa $\mathbb{Z}_5$.

Možné abelovské grupy potom dostaneme tak, že z každého bodu vezmeme jednu možnost.

- ① $\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{180}$
- ② $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{60} \times \mathbb{Z}_3$
- ③ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{90} \times \mathbb{Z}_2$
- ④ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{30} \times \mathbb{Z}_6$

Theorem

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

Důkaz.

$\Rightarrow$) *Nechť $\mathbb{Z}_m = \langle x \rangle$, $\mathbb{Z}_n = \langle y \rangle$ a l nejmenší společný násobek l.c.m. (m, n) . Všimneme si, že $l = mn$, právě když $\gcd(m, n) = 1$. Dále nechť $x^a y^b \in \mathbb{Z}_m \times \mathbb{Z}_n$ 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 $|xy| = (|x|, |y|) = mn$. Tudíž $\mathbb{Z}_m \times \mathbb{Z}_n = \langle xy \rangle$.*



Theorem

Nechť $H, K \leq G$. 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.

Nechť $x \in HK$ 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.



Theorem

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

Důkaz.

Protože $H, K \trianglelefteq G$, je $HK \leq G$. Nechť $h \in H, k \in K$. 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

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

je proto dobře definované. Že φ je homomorfismus: $h_1, h_2 \in H$ a $k_1, k_2 \in K$. Pak díky tomu, že prvky H a K spolu komutují, platí $(h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2)$ a tento tvar je jednoznačně zapsán ve tvaru hk , kde $h \in H, k \in K$. Takže

$$\begin{aligned}\varphi(h_1k_1h_2k_2) &= \varphi(h_1h_2k_1k_2) = (h_1h_2, k_1k_2) = (h_1, k_1)(h_2, k_2) = \\ &= \varphi(h_1k_1)\varphi(h_2k_2),\end{aligned}$$

tedy φ je homomorfismus a protože stejného řádu φ je isomorfismus.



Nalezení direktního součinu podgrup v grupě

V G najdeme $H, K \trianglelefteq G$ tak, že $H \cap K = e$. Potom $HK \simeq H \times K$
V abelovských grupách je ukázáno.

Jak u nekomutativních grup?

Nechť $x, y \in G$, $A, B \subseteq G$, $A, B \neq \emptyset$

Definice:

- 1 Komutátor prvků x, y je $[x, y] = x^{-1}y^{-1}xy$
- 2 Podgrupa generovaná komutátory prvků z A a B je $[A, B] = \{< [a, b] > \mid \forall a \in A, b \in B\}$
- 3 Komutátorová podgrupa $G' = \{< [x, y] > \mid \forall x, y \in G\}$

Theorem

Necht' $x, y \in G$, $H \leq G$, potom

- ① $xy = yx[x, y]$
- ② $H \trianglelefteq G \Leftrightarrow [H, G] \leq H$
- ③ $\sigma([x, y]) = [\sigma(x), \sigma(y)]$ pro všechny automorfismy $\sigma \in \text{Aut}(G)$, G' je charakteristické v G a G/G' je abelovská
- ④ G/G' je největší abelovská faktor grupa, tj. pokud $H \trianglelefteq G$ a G/H je abelovská, potom $G' \leq H$.
- ⑤ Pokud $\varphi : G \rightarrow A$ je libovolný homomorfismus do abelovské grupy A , potom $G' \leq \text{Ker } \varphi$

- 1 Z definice
- 2 $H \trianglelefteq G \Leftrightarrow ghg^{-1} \in H \Leftrightarrow \exists \bar{g} = g^{-1}, \bar{g}^{-1}h\bar{g} \in H \Leftrightarrow h^{-1}\bar{g}^{-1}h\bar{g} \in H$
- 3 Že je abelovská

$$(xG')(yG') = (xyG') = (yxx^{-1}y^{-1}G') = (yxG') = (yG')(xG')$$

- 4 $(xH)(yH) = yHxH$ dále
 $H = (xH)^{-1}(yH)^{-1}(xH)(yH) = x^{-1}y^{-1}xyH = [x, y]H$ pro všechna $x, y \in G \Rightarrow G' \leq H$. Platí i obráceně.
- 5 Protože je maximální abelovská a z předchozího důkazu.

Remark

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 HG , 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 .

Theorem

Bud' H a K grupy a $\varphi : K \rightarrow \text{Aut } H$ je homomorfismus (každému prvku $k \in K$ přiřadí nějakou permutaci H). Dále buď $\cdot$ 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:

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

- ❶ G s takto definovanou operací je grupa řádu $|G| = |K||H|$.
- ❷ Množiny $\{(h, 1) | h \in H\}$ a $\{(1, k) | k \in K\}$ jsou podgrupy G isomorfní grupám H a K . (Dále mezi nimi nerozlišujeme.)
- ❸ HG .
- ❹ $H \cap K = e$.
- ❺ $(h \in H, k \in K)(khk^{-1} = k \cdot h)$.

Důkaz.

- ❶ Asociativita platí, protože pro libovolné $(a, x), (b, y), (c, z) \in G$ platí

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

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

Example

Nechť p, q jsou prvočísla $p < q$, $|G| = pq$ a necht' $P \in \text{Syl}_p(G)$ a $Q \in \text{Syl}_q(G)$, potom

- ① $Q \trianglelefteq G$
- ② Pokud také $P \trianglelefteq G$, pak G je cyklická

Ad 1) $n_q = 1 + kq$, $n_q | p \Rightarrow n_q = 1 \Rightarrow Q \trianglelefteq G$

Ad 2) Jelikož $n_p | q$ prvočíslo, potom $n_p = 1$, nebo q . Pokud $n_p = 1$ pak $P \trianglelefteq G$, $G = PQ \simeq P \times Q \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$.

Použití Sylowovy věty: Grupa řádu 30

Example

Předpokládejme $|G| = 30$. Ukážeme, že má normální podgrupu izomorfní grupě $\mathbb{Z}_{15}$.

Každá podgrupa řádu 15 je normální a podle předchozího příkladu je abelovská, stačí dokázat, že vždy existuje taková podgrupa.

Nechť $P \in \text{Syl}_5(G)$ a $Q \in \text{Syl}_3(G)$. Je-li jedna z nich normální, pak PQ je podgrupa řádu 15. Pokud není ani jedna z nich normální, pak $n_5 = 6$ a $n_3 = 10$.

Průnik různých Sylowových podgrup řádu 5 i řádu 3 (jsou cyklické) je jednotkový element (Lagrangeova věta).

Z toho plyne že máme v tomto případě bychom potřebovali

$(6 \cdot 4) + (10 \cdot 2) = 44$ různých prvků v grupě. Nesmysl $\Rightarrow n_p \vee n_q = 1$, ale protože $PQ \trianglelefteq G$ musí být obě jsou normální, tj $n_p = n_q = 1$.

Example

Grupa řádu p^2q má normální Sylowovu podgrupu. Necht' $P \in \text{Syl}_p(G)$ a $Q \in \text{Syl}_q(G)$.

- 1 $p > q$, $n_p = 1 + kp$, $n_p | q \Rightarrow n_p = 1$ a $P \trianglelefteq G$.
- 2 $p < q$, $n_q = 1 + lq$. Pokud $n_q = 1$ je $Q \trianglelefteq G$. Pokud $n_q > 1$, $n_q | p^2$, tj. $n_q = p^2$ nebo $n_q = p$. Ale $q > p$, $\Rightarrow q = p^2$, tedy

$$lp = p^2 - 1 = (p - 1)(p + 1).$$

Jelikož $q > p$ tak $q = p + 1$ a to je možné pro $p = 2$, $q = 3$, tj. grupa řádu 12, u ostatních je $n_q = 1$ a $Q \trianglelefteq G$.

Grupa řádu $12 = 2^2 \cdot 3$ má $n_3 = 1$ nebo $n_3 = 4$. Je-li $n_3 = 4$ je to $4 \times 2 = 8$ prvků řádu 3. V tom případě Syl_2 podgrupa řádu 4 obsahuje všechny zbylé prvky a je právě jedna.

Použití Sylowovy věty: Grupa řádu 12

Example

Nechť $|G| = 12$. Ukážeme, že buď má normální Sylowovu 3-podgroupu nebo je izomorfní grupě A_4 .

Pro $n_3 = 1$ je podgrupa normální. Nechť $n_3 = 4$. Průnik Syl podgrup je e a obsahují $2 \cdot 4 = 8$ různých prvků řádu 3, $|G : N_G(P)| = n_3 = 4$. A protože P normalizuje sama sebe $N_G(P) = P$.

Vezměme akci grupy G na podmnožině $Syl_3(G)$, té odpovídá permutační reprezentace

$$\varphi : G \rightarrow S_4,$$

jádro akce nepřehazuje P_i , tudíž musí být podgrupou normalizátorů všech P_i a to je jenom e . Takže φ je injektivní.

$$G \simeq \varphi(G) \leq S_4.$$

Podgrupa řádu 12 v S_4 , která obsahuje 8 prvků řádu 3 je A_4 ,

$$\varphi(G) = A_4, \quad G \simeq A_4.$$

Použití Sylowovy věty: Grupa řádu 60

Corollary

Mějme grupu $|G| = 60$. Má-li více jak jednu Sylowovu 5–podgrupu, potom G je prostá.

Důkaz sporem.

*Nechť $n_5 > 1$ a existuje netriviální $H \trianglelefteq G$. Pak $n_p = 6$ a $|N_G(P)| = 10$
Protože index normalizátoru je počet konjugovaných.*

*Pokud $5 \mid |H|$ pak H musí obsahovat všech 6 Syl_5 podgrup
 $|H| \geq 1 + 6 \cdot 4 = 25$ a $|H| \mid 60$, takže $|H| = 30$, ale grupa řádu 30 má pouze jednu normální Syl_5 podgrupu a to je spor, tzn. $5 \nmid |H|$.*

Pokud $5 \nmid |H|$.

*Nechť $|H| = 6$ nebo 12, pak H má charakteristickou (normální) právě jednu Syl podgrupu, která je normální i v G . Vezměme jednu z char podgrup H ,
 $K \trianglelefteq H$, $|K| = 2, 3, 4$ a faktor grupu $\overline{G} = G/K$, $|\overline{G}| = 30, 20, 15$. $\overline{G}$ má normální podgrupu $\overline{L} \trianglelefteq \overline{G}$ řádu 5 dle předchozího. $L/K \trianglelefteq G/K$, 4.VOI
 $L \trianglelefteq G$ a $5 \mid |L|$. Spor $L \trianglelefteq H$.*



Závěr: A_5 je prostá. (12345) a (13425) jsou generátory různých Syl_5 podgrup.

Polopřímý součin

Polopřímý součin je další způsob, jak nebo studovat strukturu grupy nebo jak z menších grup vyrobit grupu větší jejich složením. 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 si vezmeme přímý součin. Předpokládejme, že už máme G a platí $H \cap K = e$. Dále $HK \leq G$ 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. **Důležité je, že výraz $(k_1 h_2 k_1^{-1})$ vyjadřuje zobrazení prvku h_2 automorfismem podgrupy H .** Cílem polopřímého součinu je zavést grupu s obdobným násobením bez „zastřešující“ grupy, která nám umožňuje násobit mezi sebou prvky z K a H .

Theorem

Bud'te H a K grupy a $\varphi : K \rightarrow \text{Aut } H$ je homomorfismus (každému prvku $k \in K$ přiřadí nějakou permutaci H). Dále bud' $\cdot$ 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 $(\forall h \in H, k \in K)(khk^{-1} = k \cdot h)$.

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 3. rovnosti mezi 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 .

Důkaz.

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 polopřímého součinu

Grupy G z předchozí věty nazýváme **polopřímý součin** grup H a K vzhledem k homomorfismu φ a značíme $H \rtimes_{\varphi} K$.

Theorem

Nechť $H, K \leq G$ tak, že

- ① $H \trianglelefteq G$
- ② $H \cap K = e$
- ③ $\varphi : K \rightarrow \text{Aut}(H)$ je homomorfismus levou konjugací v H , $\varphi \mapsto k \sqcup k^{-1}$

Potom $HK \simeq H \rtimes_{\varphi} K$

Speciálně : je-li $G = HK$ a jsou-li splněny podmínky 1) a 2) potom $G = H \rtimes_{\varphi} K$

Důkaz.

$H \trianglelefteq G \Rightarrow HK \leq G$, každé $x \in HK$ může být zapsáno právě jedním způsobem $x = hk$; tj. existuje bijekce

$$(hk) \mapsto (h, k), \quad HK \mapsto H \rtimes_{\varphi} K$$



Použití ke klasifikaci grup řádu n

- 1 najít $G = HK$, $H \cap K = 1$ a $H \trianglelefteq K$
- 2 pro různé páry H a K najít všechny izomorfismy
- 3 pro každý pár H, K najít homomorfismus $\varphi : K \rightarrow \text{Aut}(H)$ (homomorfismů může být více)
- 4 pro každou trojici K, φ vytvořit $H \rtimes_{\varphi} K$ a vybrat neizomorfní.

Example

- Dihedrál ní grupa $D_n \simeq \mathbb{Z}_n \rtimes_{\varphi} \mathbb{Z}_2$.
 $\varphi_s(r) = srs^{-1} = r^{-1}$, $\varphi_{s^2}(r) = \varphi_e(r) = r$
- Grupa řádu pq , $p < q$
Měli jsme $P \in \text{Syl}_p(G)$ a $Q \in \text{Syl}_q(G)$, potom $Q \trianglelefteq G$ a P a Q jsou cyklické. $\text{Aut}(Q)$ je cyklická řádu $q - 1$, tj. všechny automorfismy jsou $q^i \mapsto q^{ik}$ $k = 1, 2, \dots, q - 1$. (pro $k = 0$ není automorfismus) Pokud $p \nmid q - 1$, potom φ je pouze identita a neexistuje polopřímý součin (obraz homomorfismu do grupy $\text{Aut}(Q)$ je podgrupa), G je abelovská. Nechť $p \mid q - 1$, a $P = \langle y \rangle$ potom $\text{Aut}(Q)$ obsahuje podgrupu řádu p generovanou $\langle \gamma \rangle$ a máme množinu p homomorfismů $\varphi_k(y) = \gamma^k$, $k = 0, 1, \dots, p - 1$, přičemž $\varphi_0(y)$ je triviální a ostatní jsou izomorfní.

*Bud'ťe 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 injektivní, nazýváme takovou reprezentaci **věrnou**.*
- *Je-li $\dim V < \infty$ (existuje tedy konečná báze V), mluvíme o **maticové** reprezentaci.*

- T je vždy věrnou reprezentací faktor grupy $G/\text{Ker } T$.
- Prostá grupa má jen věrné reprezentace (kromě triviální).

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

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 je-li navíc A unitární, říkáme, že reprezentace jsou **unitárně ekvivalentní**. (izometrie : $\|A\varphi\| = \|\varphi\|$, $\forall \varphi \in V$)

Pro maticové reprezentace jde o změnu báze.

Lemma (Hilbert)

Každá maticová reprezentace grupy je ekvivalentní unitární reprezentaci.

Důkaz.

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

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

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 $j = k$). □

Důkaz.

Proto můžeme vytvořit matice $D^{\frac{1}{2}}$ a $D^{-\frac{1}{2}}$. Potom z definice zřejmě platí:

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

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

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

Tím je důkaz dokončen.



Reducibilní a ireducibilní reprezentace

$V_1 \subset V$ 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**.

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**.

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

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

Theorem

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: $(T(g)E_1 = E_1 T(g))(\forall g \in G)$.

Důkaz.

- 1 Necht' $\psi_1 \in \mathcal{H}_1$ 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

$$\langle \psi_2 | T(g)\psi_1 \rangle = 0 = \langle T^\dagger(g)\psi_2 | \psi_1 \rangle. \quad (73)$$

- 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.

$$E_1 T(g)|\psi\rangle = E_1 T(g)|\psi_1\rangle + E_1 T(g)|\psi_2\rangle = E_1 T(g)E_1|\psi\rangle = T(g)E_1|\psi\rangle. \quad (74)$$

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

Corollary (Maschke)

Reducibilní unitární reprezentace je úplně reducibilní.

Theorem

Každá unitární ireducibilní reprezentace konečné grupy má konečnou dimenzi $n \leq |G|$. $\text{Span}\{T(g_i)|\psi_1\rangle\}$, $i = 1, \dots, n$ je invariantní díky homomorfismu.

Důkaz.

$\psi_1 \in \mathcal{H}$, $\psi_\infty \neq \emptyset$



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 69 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. □

8. přednáška chybí

Geometrická interpretace Velké věty ortogonality

Velká věta ortogonality tedy říká, že pokud vytvoříme vektory čísel o počtu prvků $|G|$ tak, že si zvolíme jednu ireducibilní reprezentaci a v ní μ -tý řádek a ν -tý sloupec a prvky vektoru jsou prvky příslušné pozice v matici IR reprezentace pro všechny prvky grupy G ve stejném pořadí, pak jsou tyto vektory ortogonální pro různé pozice v matici dané reprezentace a totéž s maticemi neekvivalentních IR reprezentací. (Vždy máme stanovené pořadí prvků v G .) Je-li $|G| = n$, potom 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.)

Charaktery reprezentací

Pro maticové reprezentace zavedeme užitečnou veličinu nezávisící na bázi – tzv. charakter reprezentace.

Označme stopu matice $(T_I(g_i)) = \chi_I(g_i)$. **charakter prvku** g_i v reprezentaci T_I .

Množinu $\{\chi_I(e), \chi_I(g_1), \chi_I(g_2), \chi_I(g_3), \dots\}$ uspořádaných n -tici stop matic $T_I(g_i)$ nazveme **charakter reprezentace** T_I .

$$\chi_I(e) = n_I$$

Můžeme tvrdit:

- 1 Charaktery ekvivalentních reprezentací jsou zřejmě stejné (podobnostní transformací lze jednu reprezentaci převést na druhou)
- 2 Charaktery konjugovaných prvků jsou též stejné (z vlastností stopy), tj. prvky ve stejné konjugované třídě mají stejné charaktery.

$$G = C_1 \cup C_2 \cup C_3 \cup C_4 \cup \dots$$

$$\chi_I = \chi_I(e), \chi_I(C_2), \chi_I(C_3), \chi_I(C_4) \dots$$

Ortogonalita charakterů

Corollary

Věta ortogonality pro charaktery prvků grupy:

$$\sum_{g \in G} \chi_{\mu}(g)^* \chi_{\nu}(g) = n \delta_{\mu, \nu}. \quad (75)$$

Důkaz.

Ve velké větě ortogonality postavíme $\alpha = \beta$, $\mu = \nu$, tj. vezmeme diagonální elementy v každé matici a sečteme a $|G| = n$

$$\sum_{\mu=1}^{l_i} \sum_{\alpha=1}^{l_j} \left\{ \sum_{g \in G} T_i(g)_{\mu\mu}^* T_j(g)_{\alpha\alpha} \right\} = \frac{|G|}{l_i} \delta_{ij} \delta_{\mu\alpha} \delta_{\mu\alpha}, \quad (76)$$

$$\sum_{g_i \in G} \chi_{\mu}(g_i)^* \chi_{\nu}(g_i) = n \delta_{\nu\mu}, \quad (77)$$

$$\sum_i N_i \chi_\mu(C_i)^* \chi_\nu(C_i) = n \delta_{\nu\mu}, \quad (78)$$

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

$$\chi'_\mu(C_i) = \sqrt{\frac{N_i}{n}} \chi_\mu(C_i) \quad (79)$$

tvoří ortonormální systém, který je větší nebo roven počtu neekvivalentních ireducibilních reprezentací. □

Maticově lze zapsat:

$$Q = \begin{pmatrix} \chi_1(C_1) & \chi_1(C_2) & \chi_1(C_3) & \dots & \chi_1(C_k) \\ \chi_2(C_1) & \chi_2(C_2) & \chi_2(C_3) & \dots & \chi_2(C_k) \\ \chi_3(C_1) & \chi_3(C_2) & \chi_3(C_3) & \dots & \chi_3(C_k) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \chi_k(C_1) & \chi_k(C_2) & \chi_k(C_3) & \dots & \chi_k(C_k) \end{pmatrix}$$

$$Q' = \frac{1}{n} \begin{pmatrix} \chi_1^*(C_1)N_1 & \chi_2^*(C_1)N_1 & \chi_3^*(C_1)N_1 & \dots & \chi_k^*(C_1)N_1 \\ \chi_1^*(C_2)N_2 & \chi_2^*(C_2)N_2 & \chi_3^*(C_2)N_2 & \dots & \chi_k^*(C_2)N_2 \\ \chi_1^*(C_3)N_3 & \chi_2^*(C_3)N_3 & \chi_3^*(C_3)N_3 & \dots & \chi_k^*(C_3)N_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \chi_1^*(C_k)N_k & \chi_2^*(C_k)N_k & \chi_3^*(C_k)N_k & \dots & \chi_k^*(C_k)N_k \end{pmatrix}$$

Potom

$$(QQ') = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} = (Q'Q),$$

tj. platí také

$$\delta_{k,l} = \frac{N_k}{n} \sum_{\mu} \chi_{\mu}(C_k)^* \chi_{\mu}(C_l),$$

Jak zkonstruovat tabulku charakterů

Tabulka charakterů dává informace o ireducibilních reprezentacích.

- 1 $\chi_1(g_i) = 1$, triviální reprezentace
- 2 $\chi_\nu(e \equiv C_1) = l_\nu$, rozměru ireducibilní reprezentace
- 3 Počet ireducibilních reprezentací je roven počtu konjugovaných tříd. (ukážeme) Rozměry ireducibilních reprezentací l_ν jsou dány vztahem $\sum_\nu l_\nu^2 = n$. V mnoha případech má tato rovnice jednoznačné řešení.
- 4 Řádky v tabulce musí splňovat (ortogonalita)

$$\sum_i N_i \chi_\mu(C_i)^* \chi_\nu(C_i) = n \delta_{\nu\mu},$$

- 5 Sloupce musí splňovat ($Q Q' = Q' Q$)

$$\sum_\nu \chi_\nu(C_k)^* \chi_\nu(C_i) = \frac{n}{N_k} n \delta_{k,i},$$

- 6 Prvky uvnitř i -tého řádku splňují ($C_i \cdot C_j = \sum_k c_{ijk} C_k$, c_{ijk} – kolikrát je která třída obsažena v součinu.)

$$N_i \chi_\nu(C_i)^* N_j \chi_\nu(C_j) = l_\nu \sum_k c_{ijk} N_k \chi_\nu(C_k),$$

Dokážeme vztah 6, ostatní už jsme ukázali, nebo je triviální

Důkaz.

v každé třídě platí $X C_k X^{-1} = C_k$, pro $\forall X \in G$, tj. $X C_k = C_k X$, a totéž také pro reprezentace.

Vytvořme matici $\Gamma_k = \sum_i A_i$, $C_k \equiv \{A_1, A_2, A_3, \dots\}$.

Γ_k komutuje se všemi prvky reprezentace a podle Schurova lemmatu

$\Gamma_k = \eta_k \mathbb{I}$. Upravíme vztah pro c_{ijk} pro matice Γ_k . Protože výraz vpravo komutuje se všemi prvky, musí komutovat i výraz vlevo, tj musí obsahovat celé konjugované třídy a je takto rozložitelný.

$$\Gamma_i \Gamma_j = \sum_{A_i \in C_i} A_i \sum_{B_j \in C_j} B_j = \sum_{j,i} A_i B_j = \sum_k c_{ijk} \Gamma_k,$$

protože $A_i B_j = D_l \in C_k$. Dosazením $\eta_i \eta_j = \sum_k c_{ijk} \eta_k$. A uděláme stopu:

$$\Gamma_k = \eta_k I_\nu \text{ a také } \Gamma_k = \sum_{i=1}^{N_k} A_i = N_k \chi_\nu(C_k), \text{ tj.}$$

$$\eta_k = \frac{N_k \chi_\nu(C_k)}{I_\nu}.$$

Tabulka charakterů pro D_6

D_6 má tři konjugované třídy $E; A, B, C; D, F$

	C_1	$3C_2$	$2C_3$
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Poslední podmínka pro konstrukci tabulek říká:

$$C_2 \cdot C_2 = 3C_1 + 3C_3; \quad 3.3 = 3.1 + 3.2$$

$$C_3 \cdot C_3 = 2C_1 + C_3; \quad 2.2 = 2.1 + 1.2$$

$$C_3 \cdot C_2 = 2C_2; \quad 3.2 = 2.3$$

První je výsledek násobení tříd a vedle pro příslušný počet prvků.
Pro matice Γ platí:

$$\begin{aligned}\Gamma_3 \Gamma_2 &= (A + B + C)(D + F) = AD + AF + BD + BF + CD + CF = \\ &= B + C + C + A + A + B = 2(A + B + C) = 2\Gamma_2\end{aligned}$$

kolikrát je ireducibilní reprezentace obsažená v reducibilní

Theorem

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

$$a_{\mu} = \frac{1}{n} \sum_i N_i \chi_{\mu}(C_i)^* \chi(C_i). \quad (80)$$

Důkaz.

Rovnost $\chi(C_i) = \sum_{\nu} a_{\nu} \chi_{\nu}(C_i)$ vynásobíme $N_i \chi_{\mu}^*(C_i)$ a vysčítáme přes i – počet prvků ve třídě a použijeme ortogonalitu charakterů:

$$\sum_i N_i \chi_{\mu}^*(C_i) \chi(C_i) = \sum_{\nu} a_{\nu} \sum_i N_i \chi_{\mu}^*(C_i) \chi_{\nu}(C_i) = \sum_{\nu} a_{\nu} n \delta_{\mu, \nu} = a_{\mu} n$$



Což není nic jiného než rozklad do ortogonální báze.

Frobeniovo kritérium irreducibility

Tohoto rozkladu využijí k následující podmínce:

$$\begin{aligned}\sum_i N_i \chi^*(C_i) \chi(C_i) &= \sum_i N_i \sum_\nu a_\nu \chi_\nu^*(C_i) \sum_\mu a_\mu \chi_\mu(C_i) = \\ &= \sum_\nu \sum_\mu a_\mu a_\nu \sum_i N_i \chi_\nu^*(C_i) \chi_\mu(C_i) = \sum_\nu \sum_\mu a_\mu a_\nu n \delta_{\mu,\nu} = \sum_\mu |a_\mu|^2 n\end{aligned}$$

Corollary

Z definice je $T(g)$ ireducibilní reprezentace, právě když pro jednu hodnotu μ je $a_\mu = 1$. To jest

$$\sum_i \chi_{(\mu)}(g_i)^* \chi(g_i) = n. \quad (81)$$

Regulární reprezentace

Udělějme si tabulku násobení prvků grupy prvky inverzními:

A=		e	g_2	g_3	g_4
	e	e	g_2	g_3	g_4
	g_2^{-1}	g_2^{-1}	e	$g_2^{-1}g_3$	$\dots$
	g_3^{-1}	g_3^{-1}	$g_3^{-1}g_2$	e	$\dots$
	g_4^{-1}	g_4^{-1}	$g_4^{-1}g_2$	$g_4^{-1}g_3$	e
	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

Regulární reprezentace grupy je množina matic, kde každému prvku grupy je přiřazena matice, která má 1 v místě, kde se nachází daný prvek v tabulce 1 a všude jinde 0. Akce grupy je transitivní, tj. v každém slupci a každém řádku bude mít reprezentace prvku právě jednu jedničku.

Označí-li prvky matice v k -tém řádku a l -tém sloupci a_{kl} tak mohou psát

$$(T^{(reg)}(g_i))_{kl} = \delta(a_{kl}, g_i) = \delta(\{g_k^{-1}g_l\}, g_i),$$

δ se rozumí Kroneckerovo delta.

- Že je to maticová reprezentace:

$$\begin{aligned}\sum_k (T^{(reg)}(g_p))_{ik} (T^{(reg)}(g_r))_{kj} &= \sum_k \delta(\{g_i^{-1}g_k\}, g_p) \delta(\{g_k^{-1}g_j\}, g_r) = \\ &= \sum_k \delta(g_k, \{g_i g_p\}) \delta(\{g_k^{-1}g_j\}, g_r) = \delta(\{g_p^{-1}g_i^{-1}g_j\}, g_r) = \\ &= \delta(\{g_i^{-1}g_j\}, \{g_p g_r\}) = (T^{(reg)}(g_p g_r))_{ij}\end{aligned}$$

- Charaktery:

$$\chi^{(reg)}(e) = n, \quad \chi^{(reg)}(g_i) = 0 \text{ pokud } g_i \neq e$$

Počet neekvivalentních ireducibilních reprezentací

Theorem

Každá regulární reprezentace obsahuje každou ireducibilní reprezentaci tolikrát, kolik je její dimenze.

Důkaz.



Zajímá nás grupa, která ponechá Hamiltonian invariantní.
Nechť $\mathbf{R}$ je reálná ortogonální transformace souřadnic:

$$\mathbf{x}' = \mathbf{R}\mathbf{x}, \quad x'_i = \sum_j R_{ij} x_j$$

a inverzní transformace

$$x_i = \sum_j R_{ij}^{-1} x'_j = \sum_j R_{ji} x'_j$$

Takováto matice tvoří grupu vůči násobení.

Zavedeme grupu izometrickou s transformační grupou, jejíž prvky působí na funkce a ne na souřadnice.

$$P_R f(Rx) = f(x), \quad P_R f(x) = f(R^{-1}x) = g(x).$$

Je to grupa transformací svázána s transformací souřadnic.

$$\begin{aligned} P_S[P_R f(x)] &= P_S g(x) = g(S^{-1}x) = f[R^{-1}(S^{-1}x)] = \\ &= f[(SR)^{-1}x] = P_{SR} f(x) \end{aligned}$$

Example

Rotace kolem osy c o 90°

$$R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \quad P_R f(x, y, z) = f(x, -z, y)$$

Grupa svázána se Schrödingerovou rovnicí

Řešení stacionární Schrödingerova rovnice dané Hamiltonovým operátorem $\hat{H}$ je invariantní vůči grupě operátorů komutujícími s $\hat{H}$:

$$\hat{H}\psi = E\psi, \quad P_R\hat{H}\psi_n = P_RE_n\psi_n, \quad \hat{H}(P_R\psi_n) = E_n(P_R\psi_n).$$

Pokud komutují ψ_n a $P_R\psi_n$ jsou vlastní vektory příslušné téže vlastní hodnotě E_n - degenerace.

Díky této grupě můžeme z jednoho vlastního vektoru dopočítat další vlastní vektory příslušné každé dané vlastní hodnotě.

Atom vodíku - stavy s, p, ... se

Pokus jsou všechny degenerované hodnoty dopočítatelné z grupy symetrie - normální degenerace, jinak náhodná.

Předpokládejme, že hodnota E_n je l_n krát degenerovaná, tj. můžeme vybrat l_n ortonormálních vlastních vektorů příslušných E_n .

Akcí operátoru symetrie na vlastní vektor ψ_ν dostaneme obecně jiný vlastní vektor, který rozložíme do báze:

$$\psi_\kappa = P_R \psi_\nu = \sum_{\mu=1}^{l_n} T_n(R)_{\kappa,\mu} \psi_\mu.$$

Matice $T_n(R)_{\kappa,\mu}$ tvoří l_n rozměrnou reprezentaci grupy.

A pokud existuje vždy operátor, který transformuje vlastní vektor v kterýkoliv jiný vlastní vektor, je reprezentace ireducibilní.

Je vidět, že platí :

$$T_n(SR) = T_n(S) T_n(R)$$

a l_n vektorů ψ_ν tvoří bázi reprezentačního prostoru.

Grupa D_6 je grupou symetrie pro pohyb elektronu v poli tří protonů v rozích rovnostranného trojúhelníku.

Grupa $SO(3)$ je grupa symetrie pohybu elektronu v centrálním poli.

Zopakujme:

*V grupě G řadu 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 .*

Definice:

*Grupa se nazývá **řešitelná**, pokud existuje řada*

$$e = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \dots \trianglelefteq G_s = G$$

tak, že

$$G_i/G_{i-1}, \quad i = 0, 1, \dots, s-1 \tag{82}$$

je abelovská.

Theorem

Konečná grupa je řešitelná $\Leftrightarrow$ když pro každý dělitel $n \mid |G|$, $(n, \frac{|G|}{n}) = 1$ má grupa G podgrupu řádu n .
Pokud N a G/N jsou řešitelné, pak G je řešitelná

Důkaz.

Nechť $\overline{G} = G/N$ a $e = N_0 \trianglelefteq N_1 \trianglelefteq \dots \trianglelefteq N_r = G$ tak, že N_{i+1}/N_i je abelovská a necht' $N = \overline{G}_0 \trianglelefteq \overline{G}_1 \trianglelefteq \overline{G}_2 \dots \trianglelefteq \overline{G}_m = \overline{G}$ je řada podgrup tak, že $\overline{G}_{i+1}/\overline{G}_i$ jsou abelovské. Podle 4. VOI existuje G_i $N \leq G_i$ a podle 3. VOI

$$\overline{G_{i+1}}/\overline{G_i} \simeq G_{i+1}/G_i.$$

Tudíž

$$e = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \dots \trianglelefteq N_s = N = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \dots \trianglelefteq G_s = G$$

a všechny faktor grupy jsou abelovské.



Maximální podgrupy

Definice:

Maximální podgrupa je vlatní podgrupa $M < G$, tak že neexistuje H $M < H < G$.

Lemma

Nechť p je prvočíslo a P je grupa řádu p^a , $a \geq 1$. Potom

- ❶ $Z(P) \neq 1$
- ❷ H je netriviální normální podgrupa, potom $H \cap Z(P) \neq 1$
- ❸ Pokud $H \trianglelefteq P$ potom pro každé $p^b \mid |H|$ v H existuje normální podgrupa řádu p^b .
- ❹ Pokud $H < P$ pak $H < N_P(H)$ (nerovná se, je vlastní, jsou prvky mimo H , které normalizují H .)
- ❺ Každá maximální podgrupa P má index p .

Definice:

- 1 Grupa G , definujeme

$$Z_0(G) = 1, \quad Z_1(G) = G,$$

a Z_{i+1} je podgrupa G obsahující Z_i takto:

$$Z_{i+1}/Z_i = Z(G/Z_i)$$

(tj. Z_{i+1} je vzor centra $Z(G/Z_i)$ v G při přirozené projekci) Řada podgrup

$$Z_0(G) \leq Z_1(G) \leq \dots \leq Z_{k-1} \leq$$

se nazývá **horní centrální řada** G .

- 2 Grupa G se nazývá **nilpotentní** pokud $Z_c = G$ pro nějaké $c \in \mathbb{N}$, c je třída nilpotence G .

- Pokud G je abelovská, je nilpotentní třídy 1, protože

$$G = Z(G) = Z_1(G)$$

- Pro každou konečnou grupu existuje n tak, že

$$Z_n(G) = Z_{n+1}(G) = Z_{n+2}(G) = \dots$$

Např. $Z_n(D_6) = 1$ pro všechna $n \in \mathbb{Z}^+$

Podle definice $Z_n(G)$ je vlastní podgrupou pro všechny nilpotentní grupy.

- D_8 a Q_8 jsou nilpotentní třídy 2.

Komutátory a dolní centrální řady

Komutátor prvků x, y grupy G je definován

$$[x, y] = x^{-1}y^{-1}xy$$

a komutátor dvou podgrup H, K

$$[H, K] = \{[h, k], h \in H, k \in K\}.$$

Definice:

Pro každou grupu G definujeme následující podgrupy:

$$G^0 = G, \quad G^1 = [G, G], \quad G^{i+1} = [G, G^i].$$

*Potom řada podgrup se nazývá **dolní centrální řadou** grupy G .*

$$G^0 \geq G^1 \geq G^2 \geq \dots$$

Theorem

Grupa G je nilpotentní $\Leftrightarrow G^n = 1$ pro nějaké n . Je nilpotentní třídy $c \Leftrightarrow c$ je nejmenší číslo pro něž platí $G^c = 1$

Komutátorové řady a řešitelné grupy

Definice:

Pro každou grupu G definujme následující podgrupy:

$$G^{(0)} = G, \quad G^{(1)} = [G, G], \quad G^{(i+1)} = [G^{(i)}, G^{(i)}].$$

*Potom řada podgrup se nazývá **komutátorovou řadou** grupy G .*

$$G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \dots$$

Example

$$G = S_3, \quad G^{(1)} = G^1 = A_3, \quad G^2 = [S_3, A_3] = A_3, \quad G^{(1)} = [A_3, A_3] = 1$$

Theorem

Grupa G je řešitelná $\Leftrightarrow G^{(n)} = 1$ pro nějaké n .

Závěr: Hierarchie grup

cyklické grupy $\subset$ abelovské grupy $\subset$ nilpotentní grupy $\subset$ řešitelné grupy $\subset$
 $\subset$ všechny grupy

Grupy a reprezentace 8

Zpracováno s pomocí poznámek J. Mareše

wiki-skripta



RS

Smolka, Rudolf

MP

Paryzkova, Magdalena

SV

Vedl, Simon

TL

Leheckova, Tereza

Reprezentace grup

Reprezentace grup nám umožní

- využít matematické zákonitosti ke studiu struktury grup
- z teoretického rozboru reprezentací grup se dostaneme k ortnálním vektorům a bázím v Hilbertových prostorech.
- využití v kvantování systému

Základní definice:

*Bud' 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 injektivní, nazýváme takovou reprezentaci **věrnou**, tj. $g_i \neq g_j \Leftrightarrow T(g_i) \neq T(g_j)$.
- Je-li $\dim V < \infty$ (existuje tedy konečná báze V), mluvíme o **maticové** reprezentaci. Operátoru $T(g)$ je přiřazena matice $A(g)$ hodnosti n .



Smolka, Rudolf



Paryzkova, Magdalera



Vedl, Simon



Leheckova, Tereza

Unitární reprezentace

- T je vždy věrnou reprezentací faktor grupy $G/\text{Ker}(T)$ (1. VOI).
- Prostá grupa má jen věrné reprezentace (kromě triviální)(jádro je e).

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

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 je-li navíc A unitární, říkáme, že reprezentace jsou **unitárně ekvivalentní**. (izometrie : $\|A\varphi\| = \|\varphi\|, \forall \varphi \in V$)

Pro maticové reprezentace jde o změnu báze.

Lemma (Hilbert)

Každá maticová reprezentace grupy je ekvivalentní unitární reprezentaci.

Důkaz.

Konstrukcí: Uděláme hermitovskou, zdiagonalizujeme a z ní unitární. Nechť matice A_i reprezentuje prvek $g_i \in G$, tj. $A_i = T(g_i)$. Sestrojíme hermitovskou matici $H = \sum_{i=1}^r A_i A_i^\dagger$. Hermitovské matice můžeme diagonalizovat pomocí unitární matice U . Nechť tato diagonalizovaná matice je:

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

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

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

Členy D_{kk} jsou kladné. ($\neq 0$ protože e odpovídá jednotková matice). □

Důkaz.

Proto můžeme vytvořit matice $D^{\frac{1}{2}}$ a $D^{-\frac{1}{2}}$. Potom z definice zřejmě platí:

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

Nyní již definujeme matice finální reprezentace $A''_i = D^{-\frac{1}{2}} A'_i D^{\frac{1}{2}}$, o kterých ukážeme, že jsou unitární (ne zcela triviální):

$$\begin{aligned} A''_j A''_j{}^{\dagger} &= D^{-\frac{1}{2}} A'_j D^{\frac{1}{2}} I D^{\frac{1}{2}} A_j'^{\dagger} D^{-\frac{1}{2}} = \\ &= D^{-\frac{1}{2}} A'_j D^{\frac{1}{2}} \left[D^{-\frac{1}{2}} \sum_i A'_i A_i'^{\dagger} D^{-\frac{1}{2}} \right] D^{\frac{1}{2}} A_j'^{\dagger} D^{-\frac{1}{2}} = \\ &= D^{-\frac{1}{2}} \sum_i A'_j A'_i (A'_j A'_i)^{\dagger} D^{-\frac{1}{2}} = \\ &= D^{-\frac{1}{2}} \sum_k A'_k A_k'^{\dagger} D^{-\frac{1}{2}} = I. \end{aligned}$$

Čímž jsme zkonstruovali k dané maticové reprezentaci reprezentaci unitární.

FM

Moučka, Filip

RS

Smolka, Rudolf

MP

Paryzková, Magdalena

TL

Lehecková, Tereza

SV

Vedl, Simon

GC

Chadzitaskos, Goc

Reducibilní a ireducibilní reprezentace

Definice:

$V_1 \subset V$ 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** $V_1 \neq \vec{0}$ a V .

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 $(\forall g \in G)(T(g)(V_1) \subset V_1) \Rightarrow (V_1 = \vec{0} \vee V_1 = V)$. V opačném případě se reprezentace nazývá **reducibilní**.

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

$$T(g) = \oplus_{\mu} T^{\mu}(g)$$

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

Theorem

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 Necht' $|\psi_1\rangle \in \mathcal{H}_1$ a $|\psi_2\rangle \in \mathcal{H}_2$, pak z předpokladu máme $T(g)|\psi_1\rangle \in \mathcal{H}_1 = \mathcal{H}_2^\perp$ a platí, protože $T^{-1}(g) = T(g^{-1})$

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

- 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.

$$E_1 T(g)|\psi\rangle = E_1 T(g)|\psi_1\rangle + E_1 T(g)|\psi_2\rangle = E_1 T(g)E_1|\psi\rangle = T(g)E_1|\psi\rangle. \quad (1)$$

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

FM

Moučka, Filip

RS

Smolka, Rudolf

MP

Paryzkova, Magdalena

TL

Leheckova, Tereza

SV

Vedl, Simon

GC

Chadzitaskos, Goge

Důsledek

Corollary

Nechť T je unit. reduc. repoz. G na $\mathcal{H}$ a necht' $\mathcal{H}_1 \subset \mathcal{H}$ je invariantní podprostor.

$\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$; potom $T = T_1 \oplus T_2$ jsou reprezentace na obou podprostorech a jsou-li obě ireducibilní, pak je reprezentace úplně reducibilní. Pokud ne, opět je můžeme napsat jako direktní součet na invariantních podprostorech atd., atd..

U maticové reprezentace lze výběrem báze převést matici na blokově diagonální tvar.

$$A = \begin{pmatrix} T_1(g) & 0 & 0 & 0 & \dots \\ 0 & T_2(g) & 0 & 0 & \dots \\ 0 & 0 & T_3(g) & 0 & \dots \\ 0 & 0 & 0 & T_4(g) & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \quad (2)$$

kde jednotlivé bloky jsou ireducibilní reprezentace.

Z toho plyne:

Corollary (Maschke)

Každá reducibilní unitární reprezentace konečné grupy je úplně reducibilní.

Dokáže se postupnou aplikací předchozí věty.

Theorem

Každá unitární ireducibilní reprezentace konečné grupy má konečnou dimenzi $n \leq |G|$.

Důkaz.

$\psi_1 \in \mathcal{H}, \psi_1 \neq \vec{0}$.

$\text{Span}\{T(g_i)|\psi_1\rangle\}, i = 1, \dots, n$ je invariantní díky homomorfismu. $\square$

Theorem (1. Schurovo lemma)

Každá matice, která komutuje se všemi maticemi ireducibilní reprezentace je násobkem jednotkové matice.

(Pozn: $\Rightarrow$ platí obecně, $\Leftrightarrow$ platí pro konečné reprezentace)

Důkaz.

Víme, že se můžeme omezit je na unitární matice. Mějme tedy matici M , pro kterou platí

$$MA_i = A_i M, \quad \forall i.$$

Sdružením obou stran dostaneme a vynásobením maticí A_i zprava i zleva

$$A_i \cdot | M^\dagger A_i^\dagger = A_i^\dagger M^\dagger | \cdot A_i$$

dostaneme $A_i M^\dagger = M^\dagger A_i$, tedy i $M^\dagger$ komutuje se všemi maticemi reprezentace. Nyní můžeme vytvořit hermitovské matice $H_+ = M + M^\dagger$ a $H_- = i(M - M^\dagger)$ a vyjádřit $M = H_+ - iH_-$. Potom M je konstantní právě tehdy, když tyto hermitovské matice jsou konstantní, a proto se můžeme omezit na hermitovské komutující matice H . □

Důkaz.

Hermitovskou matici můžeme diagonalizovat, tedy $D = U^{-1}HU$ a definujeme $A'_i = U^{-1}A_iU$. Potom platí $A'_iD = DA'_i$ díky invarianci maticových rovnic vůči unitárním transformacím. Nyní musíme ukázat, že D je nejen diagonální, ale přímo násobkem jednotkové matice. Napíšeme po složkách

$$(A'_i)_{\mu\nu}d_{\nu\nu} = d_{\mu\mu}(A'_i)_{\mu\nu}, \quad (A'_i)_{\mu\nu}(d_{\nu\nu} - d_{\mu\mu}) = 0.$$

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 $\forall\mu, \forall\nu$. □

Theorem (2. Schurovo lemma)

Máme-li dvě ireducibilní reprezentace T_1 a T_2 rozměru l_1 a l_2 téže grupy G na $\mathcal{H}_1$ a $\mathcal{H}_2$ a dále necht' existuje obdélníková matice M , pro kterou platí:

$$MT_1(g) = T_2(g)M, \quad \forall g \in G$$

a

- ① *pokud $(l_1 \neq l_2)$ potom $M = 0$ (nulová matice)*
- ② *pokud $l_1 = l_2$ 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.*

Matice M má l_1 sloupců a l_2 řádků.

Důkaz.

Opět uvažujeme pouze unitární matice a bez újmy na obecnosti nechť $l_1 \leq l_2$. Nyní sdružením rovnice pro M dostaneme:

$$T_1(g)^\dagger M^\dagger = M^\dagger T_2(g)^\dagger, \quad T_1(g^{-1})M^\dagger = M^\dagger T_2(g^{-1}).$$

Nyní obě strany vynásobíme zprava M a využijeme toho, že rovnost platí pro všechny g_i^{-1} stejně jako pro všechna g_i . Dostaneme (použitím předpokladu)

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

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



Důkaz.

Uvažujme nejprve $l_1 = l_2$, tedy M je čtvercová matice. Pomocí pravidel počítání determinantů máme $(\det M)^2 = c^{l_1}$. Nyní pokud $c \neq 0$, musí mít M nenulový determinant. V případě, že $c = 0$ máme $MM^\dagger = 0$. Po složkách tedy

$$\sum_{\alpha} M_{\mu\alpha} M_{\alpha\nu}^\dagger = \sum_{\alpha} M_{\mu\alpha} M_{\nu\alpha}^* = 0, \quad \forall \mu, \nu.$$

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 se M přidáním $l_2 - l_1$ nulových sloupců na čtvercovou matici N . Platí, že $NN^\dagger = MM^\dagger$. Jelikož N má zřejmě nulový determinant, dostáváme případ, kdy $M = 0$. □

Relace ortogonality z teorie reprezentací



Theorem (velká věta ortogonality)

Uvažujme všechny neekvivalentní ireducibilní unitární reprezentace grupy G . Platí:

$$\sum_{g \in G} T_i(g)_{\mu\nu}^* T_j(g)_{\alpha\beta} = \frac{|G|}{l_i} \delta_{ij} \delta_{\mu\alpha} \delta_{\nu\beta}, \quad (3)$$

kde l_i je rozměr reprezentace T_i .



FM

Moučka, Filip

RS

Smolka, Rudolf

MP

Paryzková, Magdalena

TL

Lehecková, Tereza

SV

Vedl, Simon

GC

Chadzitaskos, Goc

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 tranzitivnost grupy a ukážeme komutativitu M :

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

FM

Moučka, Filip

RS

Smolka, Rudolf

MP

Paryzková, Magdalena

TL

Lehecková, Tereza

SV

Vedl, Simon

GC

Chadzitaskos, Goc

Důkaz.

Musí tedy platit, že $M = 0$, tedy

$$M_{\alpha\mu} = 0 = \sum_g \sum_{\kappa\lambda} T_2(g)_{\alpha\kappa} X_{\kappa\lambda} T_1(g^{-1})_{\lambda\mu}. \quad (5)$$

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:

$$0 = \sum_g T_2(g)_{\alpha\beta} T_1(g^{-1})_{\nu\mu} = \sum_g T_2(g)_{\alpha\beta} T_1(g)^*_{\mu\nu}, \quad (6)$$

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

Důkaz.

Nyní mějme jednu reprezentaci a znovu zkonstruujeme matici M jako:

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

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 .



Důkaz.

Nyní zvolíme $\mu = \mu'$ a sečteme přes diagonálu.

$$\sum_g T_1(gg^{-1})_{\nu'\nu} = l_1 c_{\nu\nu'},$$

$$\sum_g T_1(gg^{-1})_{\nu'\nu} = \sum_g T_1(e)_{\nu'\nu} = |G| \delta_{\nu\nu'}.$$

Odtud máme $c_{\nu\nu'} = \frac{|G|\delta_{\nu\nu'}}{l_1}$ (Závisí na řádu grupy a dimenzi reprezentace).
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. □