# Grupy a reprezentace 5

Zpracováno na základě poznámek J. Mareše a s jejich využitím

wiki-skripta

# Hölderův program 1880

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 – Thopsonova 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 isomorfní 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 publikovám v r 1963 a byl na 255 stranách matematických výpočtů.* □

# Některé příklady

## 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 $S_n \longrightarrow \{-1, 1\}$
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 $\sim 8.10^{53}$

# Akce grupy na množině

Pro analýzu grup použijeme také akci grupy.

***Akcí grupy*** $G$ ***na množině*** $A$ *nazveme zobrazení* $\cdot : G \times A \to A$ *(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

*Buď* $\cdot$ *akce grupy* $G$ *na množině* $A$*. Zaveďme pro pevně zvolené* $g \in G$ *zobrazení* $\sigma_g : A \to A$ *vztahem* $(\sigma_g(a) = g \cdot a)(\forall a \in A)$*. Potom platí:*

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

## Důkaz.

1) Platí triviálně
2) Dokážeme, žeb je to homomorfismus: $\sigma_g$ 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 $S_A$.*

# Permutační reprezentace

## 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 objevé právě jednou.*

Označíme–li jednotivé 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 $G \to S_A$ je injektivní, nazvýváme reprezentaci **věrnou.**
2. Každý homohorfismus $G \to S_A$, $A \neq \emptyset$ 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 $G/\mathrm{Ker}\ \varphi$.

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

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

1. Definujeme **jádro** akce jako: $\text{Ker}\,(\cdot) = \{g \in G | g \cdot s = s \text{ pro } \forall s \in S\}$.
2. Nechť $s \in A$ je pevně zvolený prvek. Potom **stabilizátor** $s$ v $G$ je: $G_s = \{g \in G | g \cdot s = s\}$.
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 $y \in G_a$: $a = e \cdot a = (y^{-1}y) \cdot a = [$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 $G_a$.* □

## Corollary

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

$$\text{Ker}\,(\cdot) = \bigcap_{a \in A} G_a. \tag{1}$$

## Theorem (Rozklad grup díky akci)

*Nechť grupa $G$ působí akcí na množině $A$, potom:*

1. *Relace 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*

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

*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 $C_a \to gG_a$ 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 $e$.

# Akce na levých třídách

## Theorem

*Buď $H \leq G$, akce $G$ působí na levých třídách $\{g_i H\}_i = A$ a $\pi_H$ 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.*

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

## Důkaz.

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

# Cayleyho věta

**Theorem (Cayley)**

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

**Důkaz.**

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

## Corollary

*Buď $p$ nejmenší prvodělitel $|G|$ ($G$ 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 prvodělitel, 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 $G \times G \to G,\ g : a \mapsto gag^{-1}$ a je to akce $G$ na $G$.

*Buďte $G$ 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

*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 $\alpha$, 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. $P/Z(P) =< xZ(P) >$. 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. □

## Corollary

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

## Důkaz.

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

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

□

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

# Grupa automorfismů

## Theorem

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

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

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

## Důkaz.

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

*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. $\sigma \in Aut(G) \Rightarrow \sigma(H) = H$
Vlastnosti:

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

# p–grupa a Sylowowa podgrupa

*Definice: Buďte $G$ grupa a $p$ prvočíslo.*

1. *Grupu řádu $p^\alpha$ pro nějaké $\alpha \geq 1$ se nazývá **p-grupa**. Podgrupy $G$ řádu $p^\alpha$ nazýváme **p-podgrupy** $G$.*
2. *Je-li $G$ řádu $p^\alpha m$ a $p \nmid m$, pak podgrupu řádu $p^\alpha$ 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 $P \in Syl_p(G)$ a $Q$ libovolná p-podgrupa $G$, pak $N_G(P) \cap Q = P \cap Q$.*

## Důkaz.

$\supset$) *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.*
$\subset$) *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 $H \leq P$.* □

# Sylowowa věta

## Theorem (Sylow)

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

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

# Důkaz 1

Důkaz provedeme úplnou indukcí na $|G|$, přičemž pro $|G| = 1$ není co dokazovat. Nechť tedy existuje Sylowova $p$-podgrupa pro všechny grupy menšího řádu než $|G|$.
Když $p \mid |Z(G)|$, pak podle 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 $p \nmid |Z(G)|$.

# Pokračování

$p \nmid |Z(G)|$
Nechť $g_1, g_2, \ldots, g_r$ jsou reprezentanti různých tříd neobsažených v centru G, pak platí rovnice tříd

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|. \tag{2}$$

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

$$|G : C_G(g_i)| = \frac{p^\alpha m}{p^\alpha k}, \ |H| = p^\alpha k, \quad \text{kde } p \nmid k, \tag{3}$$

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 Sylovova $p$-podgrupa $G$.

# Důkaz 2 a 3

Nechť $Q$ je libovolná $p$-podgrupa G a nechť

$$\mathcal{S} = \{gPg^{-1} | g \in G\} \overset{ozn.}{=} \{P_1, P_2, \ldots, P_r\} = \mathcal{S}. \tag{4}$$

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

$$\mathcal{S} = O_1 \cup O_2 \cup \cdots \cup O_s \tag{5}$$

kde $r = |O_1| + |O_2| + \cdots + |O_s|$. 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

$$|O_i| = |Q : P_i \cap Q|, \quad 1 \leq i \leq s. \tag{6}$$

# Pokračování

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

$$|O_1| = 1, \tag{7}$$

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

$$|O_i| = |P_1 : P_1 \cap P_i| > 1, \quad 2 \leq i \leq s. \tag{8}$$

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

$$p \mid |O_i|, \quad 2 \leq i \leq s. \tag{9}$$

Odtud

$$r = |O_1| + (|O_2| + \cdots + |O_s|) \equiv 1 (mod\ p) \tag{10}$$

Nyní buď $Q$ libovolná $p$-podgrupa G. Kdyby $Q \notin P_i, \forall i \in \hat{r}$, pak $Q \cap P_i < Q, \forall i$, tedy

$$|O_i| = |Q : Q \cap P_i| > 1, \quad 1 \leq i \leq s. \tag{11}$$

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

# Pokračování

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 $\mathcal{S} = Syl_p(G)$ protože každá Sylowova $p$-podgrupa je konjugovaná k $P$, tedy $n_p = r \equiv 1 \mod p$. Nakonec díky počtu trid ekvivalence a tomu, že všechny Sylowovy $p$-podgrupy jsou konjugované, dostáváme

$$n_p = |G : N_G(P)|, \quad \forall P \in Syl_p(G). \tag{12}$$

## Corollary

*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 $\tilde{P} \in Syl_p(G)$. Pak $\tilde{P} = gPg^{-1} = P$. □