**Věta (druhá Sylowova).** *Nechť $G$ je konečná grupa, $p$ prvočíslo a $k \in \mathbb{N}$ takové, že $|G| = p^k \cdot m$ a $p \nmid m$. Označme $r$ počet $p$-Sylowských podgrup grupy $G$ (tedy podgrup grupy $G$ řádu $p^k$). Pak platí*

- $r \equiv 1 \pmod{p}, \quad r \mid m;$
- *libovolná podgrupa grupy $G$, jejíž řád je mocnina $p$, je podgrupou některé $p$-Sylowské podgrupy grupy $G$;*
- *jestliže $H$, $K$ jsou $p$-Sylowské podgrupy grupy $G$, pak existuje $g \in G$ tak, že předpis $h \mapsto g \cdot h \cdot g^{-1}$ určuje izomorfismus $H \to K$.*

**Důkaz.** Pro libovolnou podgrupu $H \leq G$ a libovolné $g \in G$ budeme užívat označení $g \cdot H \cdot g^{-1} = \{g \cdot h \cdot g^{-1};\, h \in H\}$.

Z první Sylowovy věty víme, že alespoň jedna $p$-Sylowská podgrupa grupy $G$ existuje, jednu pevně zvolme a označme ji $P$. Je tedy $P \leq G$, $|P| = p^k$. Označme

$$X = \{g \cdot P \cdot g^{-1};\, g \in G\}, \qquad s = |X|.$$

Definujme zobrazení $\varphi : G \to \mathbb{S}(X)$ předpisem: pro každé $a \in G$ a každé $P' \in X$ klademe

$$\varphi(a)(P') = a \cdot P' \cdot a^{-1}.$$

Protože $P' = g \cdot P \cdot g^{-1}$ pro nějaké $g \in G$, je

$$a \cdot P' \cdot a^{-1} = a \cdot g \cdot P \cdot g^{-1} \cdot a^{-1} = (a \cdot g) \cdot P \cdot (a \cdot g)^{-1} \in X.$$

Je tedy $\varphi(a) : X \to X$ zobrazení. Protože pro libovolná $a, b \in G$ máme

$$\begin{aligned}\varphi(a)\big(\varphi(b)(P')\big) &= \varphi(a)(b \cdot P' \cdot b^{-1}) = a \cdot b \cdot P' \cdot b^{-1} \cdot a^{-1} = \\ &= (a \cdot b) \cdot P' \cdot (a \cdot b)^{-1} = \varphi(a \cdot b)(P'),\end{aligned}$$

platí $\varphi(a) \circ \varphi(b) = \varphi(a \cdot b)$. Proto

$$\begin{aligned}\varphi(a^{-1}) \circ \varphi(a) &= \varphi(a^{-1} \cdot a) = \varphi(1) = \mathrm{id}_X, \\ \varphi(a) \circ \varphi(a^{-1}) &= \varphi(a \cdot a^{-1}) = \varphi(1) = \mathrm{id}_X,\end{aligned}$$

a tedy je $\varphi(a)$ bijekce, tudíž $\varphi(a) \in \mathbb{S}(X)$. Navíc jsme už ukázali, že je $\varphi$ homomorfismus. Je tedy $\varphi$ akce grupy $G$ na množině $X$. Označme $S_P$ stabilizátor prvku $P$ v akci $\varphi$, tedy

$$S_P = \{g \in G;\, g \cdot P \cdot g^{-1} = P\}.$$

Z definice je vidět, že množina $X$ je orbitou prvku $P$. Protože počet prvků orbity je index stabilizátoru, platí

$$s = |X| = |G/S_P| = \tfrac{|G|}{|S_P|},$$

tedy $s \cdot |S_P| = |G|$, tj. $s \mid |G|$.

Přerušme důkaz věty, abychom dokázali

**Lemma.** *Nechť $Q$ je libovolná podgrupa grupy $G$ taková, že $|Q| \mid p^k$, tj. řád $Q$ je mocnina $p$. Pak platí $Q \cap S_P = Q \cap P$. (Ekvivalentně lze lemma formulovat takto: platí $P \subseteq S_P$ a pro každý prvek $x \in S_P$ takový, že řád $x$ je mocninou $p$, platí $x \in P$.)*

**Důkaz lemmatu.** Zřejmě pro každé $g \in P$ platí $g \cdot P \cdot g^{-1} \subseteq P$. Protože předpis $x \mapsto g{\cdot}x{\cdot}g^{-1}$ zadává bijekci na $G$ (vždyť jde o vnitřní automorfismus), je $|g \cdot P \cdot g^{-1}| = |P|$, a tedy $g \cdot P \cdot g^{-1} = P$. Dostali jsme, že $P \subseteq S_P$, odkud plyne $Q \cap P \subseteq Q \cap S_P$.

Označme $H = Q \cap S_P$. Pro důkaz opačné inkluze (a tedy dokončení důkazu lemmatu) stačí ukázat, že platí $H \subseteq P$. Označme $K = \langle H \cup P \rangle$. Protože $H \cup P$ je neprázdná podmnožina $G$ obsahující s každým svým prvkem i prvek k němu inverzní, platí

$$K = \big\{a_1 \cdot a_2 \cdots a_n;\ n \in \mathbb{N},\ \forall i \in \{1, \ldots, n\}\colon a_i \in H \cup P\big\}.$$

Pro libovolné $b \in H$ z definice plyne $b \in S_P$, a tedy $b \cdot P \cdot b^{-1} = P$, a proto pro každé $a \in P$ existuje $\bar{a} \in P$ splňující $\bar{a} = b \cdot a \cdot b^{-1}$, tj. $\bar{a} \cdot b = b \cdot a$. Proto

$$K = \{a \cdot b;\ a \in P,\ b \in H\}.$$

Ukážeme nyní, že platí $|P/(H \cap P)| = |K/H|$, a to tak, že sestrojíme bijekci $f\colon P/(H \cap P) \to K/H$. Pro libovolné $a \in P$ položíme

$$f(a \cdot (H \cap P)) = a \cdot H.$$

Pro libovolné $a_1, a_2 \in P$ platí $a_1 \cdot (H \cap P) = a_2 \cdot (H \cap P)$, právě když $a_2^{-1} \cdot a_1 \in H \cap P$, což nastane, právě když $a_2^{-1} \cdot a_1 \in H$, tj. právě když $a_1 \cdot H = a_2 \cdot H$. Je tedy zobrazení $f$ nejen korektně definováno, ale také injektivní. Protože libovolné $k \in K$ je tvaru $k = a \cdot b$ pro vhodná $a \in P$, $b \in H$ a protože platí $k \cdot H = (a \cdot b) \cdot H = a \cdot H$, je $f$ také surjektivní.

Dostali jsme, že

$$\tfrac{|P|}{|H \cap P|} = |P/(H \cap P)| = |K/H| = \tfrac{|K|}{|H|},$$

a tedy

$$|K| = \tfrac{|H| \cdot |P|}{|H \cap P|}$$

je mocnina $p$. Přitom $P \subseteq K$ a $P$ je $p$-Sylowská, a tedy její řád je největší mocnina $p$ dělící $|G|$, z Lagrangeovy věty $|K| \mid |G|$, celkem tedy $P = K$. Odtud $H \subseteq K = P$ a důkaz lematu je hotov.

**Pokračování důkazu věty.** Zúžením homomorfismu $\varphi$ na libovolnou podgrupu $Q$ grupy $G$ dostaneme homomorfismus $\varphi|_Q \colon Q \to \mathbb{S}(X)$, což je akce podgrupy $Q$ na $X$.

Nejprve tuto akci studujme pro podgrupu $P$. Orbita obsahující $P$ v akci $\varphi|_P$ je rovna $\{g \cdot P \cdot g^{-1};\, g \in P\} = \{P\}$. Pro libovolné $P' \in X$, $P' \neq P$, platí, že stabilizátor $P'$ v akci $\varphi|_P$ obsahuje právě ty prvky $y \in P$, které splní

$$y \cdot P' \cdot y^{-1} = P'.$$

Přitom existuje $g \in G$, že $P' = g \cdot P \cdot g^{-1}$. Je tedy

$$\begin{aligned} y \cdot P' \cdot y^{-1} = P' &\iff y \cdot g \cdot P \cdot g^{-1} \cdot y^{-1} = g \cdot P \cdot g^{-1} \\ &\iff g^{-1} \cdot y \cdot g \cdot P \cdot g^{-1} \cdot y^{-1} \cdot g = P \\ &\iff g^{-1} \cdot y \cdot g \in S_P \\ &\iff y \in g \cdot S_P \cdot g^{-1}. \end{aligned}$$

Proto je stabilizátor $P'$ v akci $\varphi|_P$ roven $(g \cdot S_P \cdot g^{-1}) \cap P$. Přitom (uvědomte si, že předpis $x \mapsto g^{-1} \cdot x \cdot g$ zadává vnitřní automorfismus, a tedy bijekci na množině $G$)

$$|(g \cdot S_P \cdot g^{-1}) \cap P| = |S_P \cap (g^{-1} \cdot P \cdot g)|.$$

Protože je $g^{-1} \cdot P \cdot g$ podgrupa $G$ řádu $p^k$, podle lemmatu

$$S_P \cap (g^{-1} \cdot P \cdot g) = P \cap (g^{-1} \cdot P \cdot g).$$

Proto stabilizátor prvku $P'$ v akci $\varphi|_P$

$$\begin{aligned} (g \cdot S_P \cdot g^{-1}) \cap P &= g \cdot \big(S_P \cap (g^{-1} \cdot P \cdot g)\big) \cdot g^{-1} = \\ &= g \cdot \big(P \cap (g^{-1} \cdot P \cdot g)\big) \cdot g^{-1} = \\ &= (g \cdot P \cdot g^{-1}) \cap P = \\ &= P' \cap P. \end{aligned}$$

Protože počet prvků v orbitě je index stabilizátoru, má orbita obsahující $P'$ právě $|P/(P' \cap P)|$ prvků. To je ovšem mocnina $p$ větší než 1, neboť $|P' \cap P| < |P|$, vždyť $P$ a $P'$ jsou různé množiny o stejném počtu prvků. Celá množina $X$ se v akci $\varphi_P$ rozložila na několik orbit, z nichž jediná orbita $\{P\}$ je jednoprvková a všechny ostatní mají počet prvků dělitelný $p$. Proto $s = |X| \equiv 1 \pmod{p}$. Ze dříve zjištěného $s \mid |G| = p^k \cdot m$ pak plyne $s \mid m$.

Dokažme nyní sporem, že každá podgrupa grupy $G$, jejíž řád je mocnina $p$, je podgrupou některé z podgrup z množiny $X$. Předpokládejme tedy, že $Q$ je podgrupa grupy $G$, že její řád je mocnina $p$ a že $Q$ není podgrupou žádné

z podgrup z množiny $X$. Máme akci $\varphi|_Q$ podgrupy $Q$ na $X$. Stejnou úvahou jako výše určíme, že pro libovolné $g \in G$ je stabilizátor prvku $P' = g \cdot P \cdot g^{-1}$ v akci $\varphi|_Q$ roven $(g \cdot S_P \cdot g^{-1}) \cap Q$. Užitím lemmatu

$$\begin{aligned}|(g \cdot S_P \cdot g^{-1}) \cap Q| = |S_P \cap (g^{-1} \cdot Q \cdot g)| = |P \cap (g^{-1} \cdot Q \cdot g)| = \\ = |(g \cdot P \cdot g^{-1}) \cap Q| = |P' \cap Q| < |Q|,\end{aligned}$$

neboť $Q \not\subseteq P'$. Proto v akci $\varphi|_Q$ je počet prvků v každé orbitě mocnina $p$ větší než 1, tedy dělitelná $p$. Proto i součet těchto počtů $s = |X|$ je dělitelný $p$, spor.

Speciálně tedy každá $p$-Sylowská podgrupa $H$ grupy $G$ je podgrupou některé z podgrup z množiny $X$, tedy podgrupou podgrupy $g \cdot P \cdot g^{-1}$ pro vhodné $g \in G$. Protože $|g \cdot P \cdot g^{-1}| = p^k = |H|$, platí $H = g \cdot P \cdot g^{-1} \in X$. Množina $X$ proto obsahuje všechny $p$-Sylowské podgrupy grupy $G$ a $r = s$.

Jsou-li $H$ a $K$ libovolné $p$-Sylowské podgrupy grupy $G$, existují $g_1, g_2 \in G$ tak, že $H = g_1 \cdot P \cdot g_1^{-1}$, $K = g_2 \cdot P \cdot g_2^{-1}$. Položme $g = g_2 \cdot g_1^{-1}$, pak předpis $x \mapsto g \cdot x \cdot g^{-1}$, zadávající vnitřní automorfismus grupy $G$, zadává též izomorfismus $H \to K$.

Věta je dokázána.