2.B Homomorfismy a normální podgrupy

Velmi podobně jako u pologrup (a konečných grup) existují v grupách obecně podgrupy generované podmnožinami.

Lemma 2.17 *Ať je X podmnožina grupy G. Pak existuje $\langle X\rangle$ v uspořádání inkluzí nejmenší podgrupa G obsahující X.*

Důkaz. 1) První metoda důkazu je založena na faktu, že průnik (i nekonečného) systému podgrup je opět podgrupa. Pro H_i, $i \in I$, položme $H = \bigcap_{i\in I} H_i$. Neutrální prvek 1 náleží každému H_i a tedy $1 \in H$. Máme-li $g, h \in H$, pak je $g, h \in H_i$ pro všechna $i \in I$ a tedy je $gh, g^{-1}, h^{-1} \in H_i$ pro všechna i a tedy také $gh, g^{-1}, h^{-1} \in H$. Hledanou podgrupu získáme, položíme-li $\langle X\rangle = \bigcap_{H \text{ podgrupa } G,\ X\subseteq H} H$.

2) Podgrupu $\langle X\rangle$ lze zkonstruovat pomocí obecného tvaru jejích prvků. Položme $\langle X\rangle = \{x_1^{e_1} \cdot x_2^{e_2} \cdot \ldots \cdot x_n^{e_n}\ ;\ n \in \mathbb{N} \cup \{0\},\ x_i \in X \text{ a } e_i \in \{1, -1\} \text{ pro } i = 1, \ldots, n\}$. Je-li $n = 0$, pak odpovídající prázdné slovo považujeme za zápis neutrálního prvku grupy G. Obsahuje-li H podgrupa G množinu X, pak musí obsahovat i $\langle X\rangle$. Pro $x_1^{e_1} \cdot x_2^{e_2} \cdot \ldots \cdot x_n^{e_n}$ a $y_1^{e'_1} \cdot y_2^{e'_2} \cdot \ldots \cdot y_m^{e'_m}$ prvky $\langle X\rangle$ je $x_1^{e_1} \cdot x_2^{e_2} \cdot \ldots \cdot x_n^{e_n} \cdot y_1^{e'_1} \cdot y_2^{e'_2} \cdot \ldots \cdot y_m^{e'_m}$ opět prvek $\langle X\rangle$. Zbývá uzavřenost na inverze:

$$(x_1^{e_1} \cdot x_2^{e_2} \cdot \ldots \cdot x_{n-1}^{e_{n-1}} \cdot x_n^{e_n})^{-1} = x_n^{-e_n} \cdot x_{n-1}^{-e_{n-1}} \cdot \ldots \cdot x_2^{-e_2} \cdot x_1^{-e_1} \in \langle X\rangle.$$

□

Podgrupa $\langle X\rangle$ se nazývá podgrupa *generovaná* množinou X a X se nazývá *množina generátorů* grupy $\langle X\rangle$. Použili jsme stejné značení $\langle X\rangle$ pro podpologrupu i podgrupu generovanou X. Toto značení splývá v konečných grupách, ale obecně jsou to dva různé pojmy. V dalším textu bude vždy jasné, zda půjde o grupové nebo o pologrupové generování.

Úkol. Jaká je nejmenší velikost množin generátorů grup S_3, S_4 a S_5? Dá se tento výsledek rozšířit na S_n pro libovolné $n \in \mathbb{N}$?
Jaké množiny generátorů má grupa $\mathbb{Q}(+)$ racionálních čísel se sčítáním?

Homomorfismy mezi grupami zachovávají nejen násobení, ale i jednotku a inverze. Ať jsou G a H grupy a $f : G \to H$ homomorfismus. Pro $1 = 1_G \in G$ a $a \in G$ máme $f(a) = f(1 \cdot a) = f(1) \cdot f(a)$. Prvek $f(a)$ má v H inverzi $f(a)^{-1}$ a můžeme krátit $1_H = f(a) \cdot f(a)^{-1} = f(1) \cdot f(a) \cdot f(a)^{-1} = f(1)$. Tedy f zachovává neutrální prvek a pro inverze platí:

$$f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}) = f(1_G) = 1_H = f(1_G) = f(a^{-1} \cdot a) = f(a^{-1}) \cdot f(a),$$

tedy $f(a^{-1}) = f(a)^{-1}$.

Izomorfismy přenášejí všechny vlastnosti definované pomocí násobení. Například je-li grupa H izomorfní grupě G s n generátory, pak má H také n-prvkovou množinu generátorů, a podobně. Izomorfní grupy budeme značit $G \cong H$.

Značení a poznámka. Pro $A, B \subseteq S$ podmnožiny pologrupy S označme $A \cdot B = \{a \cdot b\ ;\ a \in A,\ b \in B\}$, tedy součin podmnožin po prvcích. Pro $A = \{a\}$ jednoprvkovou množinu budeme značení zkracovat $A \cdot B = a \cdot B$ a $B \cdot A = B \cdot a$, což odpovídá zápisu pravých a levých rozkladových tříd prvku podle podgrupy.

Označme $\mathrm{P}(S) = \{A\ ;\ A \subseteq S\}$ množinu všech podmnožin S, takzvanou *potenci* množiny S. Je-li S pologrupa, pak je $\mathrm{P}(S)$ s právě definovaným násobením opět pologrupa. Totiž $A \cdot (B \cdot C) = \{a \cdot b \cdot c\ ;\ a \in A,\ b \in B,\ c \in C\} = (A \cdot B) \cdot C$.

Definice. Ať je H podgrupa grupy G. Pokud pro každé $g \in G$ platí $g \cdot H = H \cdot g$, tedy pravá rozkladová třída se rovná levé, pak se H nazývá *normální podgrupa* G a značí se $H \triangleleft G$.

V pologrupě $\mathrm{P}(G)$ definované na potenci grupy G komutují normální podgrupy G se všemi prvky, tedy $H \cdot A = A \cdot H$ pro $H, A \in \mathrm{P}(G)$, $H \triangleleft G$.

Kongruence a faktorizace grup. Ekvivalence $\sim$ na grupě G se nazývá *kongruence*, pokud pro každé $g_1, g_2, h_1, h_2 \in G$ takové, že $g_1 \sim g_2$ a $h_1 \sim h_2$, platí $g_1 \cdot h_1 \sim g_2 \cdot h_2$. Jedná se o rozšíření definice kongruence na celých číslech. Budeme postupovat podobně jako v $\mathbb{Z}$. Ukážeme, že každá kongruence je jednoznačně určená třídou neutrálního prvku $[1]_\sim$. Pro prvky $g, k \in G$ platí $g \sim k$ právě když $1 \sim g^{-1}k$ (neboť $g^{-1} \sim g^{-1}$ a $g \sim g$). Tedy $g \sim k$ právě když $k = g \cdot h$, kde $h \sim 1$ (h samozřejmě musí být rovno $g^{-1}k$). Podobně $g \sim k$ právě když $1 \sim k \cdot g^{-1}$ a tak $g \sim k$ právě když $k = h \cdot g$, kde $h \sim 1$. Označme $H = [1]_\sim$. Vidíme, že pro třídu g platí $[g]_\sim = g \cdot H = H \cdot g$. Zbývá ukázat, že H je podgrupa: pro $h \in H$ platí $H = [h]_\sim = h \cdot H$ a tedy H je uzavřená na násobení. Dále je $1 \in H$ a podle předchozího $h \sim 1$ právě když $1 \sim h^{-1} \cdot 1 = h^{-1}$.

Naopak víme, že relace $\sim_H$, jejíž třídy jsou pravé rozkladové třídy podle H, je ekvivalence pro H podgrupu G. Předpokládejme, že $H \triangleleft G$. Pak pro $g_1, g_2, h_1, h_2 \in G$ takové, že $g_1 \sim_H g_2$ a $h_1 \sim_H h_2$, platí $g_1h_1H = g_1h_2H = g_1Hh_2 = g_2Hh_2 = g_2h_2H$ a tedy $g_1h_1 \sim_H g_2h_2$ a $\sim_H$ je kongruence na G. Dokázali jsme, že

kongruence odpovídají přesně normálním podgrupám.

Opět, podobně jako v $\mathbb{Z}$, lze *faktorizovat podle kongruence*, neboli *faktorizovat podle normální podgrupy*. Ať je H normální podgrupa grupy G. Pro gH a kH (pravé) rozkladové třídy máme $gH \cdot kH = gHkH = gkHH = (gk)H$, kde poslední rovnost plyne například z toho, že $1 \in H$ a H je uzavřená na násobení. Součin dvou rozkladových tříd podle H je tedy opět rozkladová třída podle H. Množina $G/H = \{gH\ ;\ g \in G\}$ všech rozkladových tříd G podle H je podpologrupa pologrupy $\mathrm{P}(G)$ potence G. Dále máme $H \cdot gH = HgH = gHH = gH = gH \cdot H$ a třída H je neutrální prvek pologrupy G/H. Nakonec $gH \cdot g^{-1}H = gHg^{-1}H = gg^{-1}HH = 1 \cdot H = H = g^{-1}H \cdot gH$ a tudíž v G/H existují inverze. Množina G/H spolu s násobením tříd je grupa a nazývá se *faktorová grupa G podle H*, nebo krátce *faktor G podle H*.

Označme $p : G \to G/H$, kde $H \triangleleft G$, zobrazení, které prvku přiřadí jeho rozkladovou třídu, tedy $p(g) = gH$. Snadno zjistíme, že p je homomorfismus: $p(gh) = ghH = ghHH = gHhH = p(g) \cdot p(h)$. Homomorfismus p se nazývá *přirozená projekce*. Je

zřejmé, že $H = p^{-1}(1_{G/H})$.

Definice. Ať je $f : G \to \overline{G}$ homomorfismus grup. Množina $\mathrm{Ker}(f) = \{a \in G\ ;\ f(a) = 1_{\overline{G}}\}$ se nazývá *jádro* homomorfismu f, množina $\mathrm{Im}(f) = \{b \in \overline{G}\ ;\ b = f(a)$ pro nějaké $a \in G\}$ se nazývá *obraz* f.

Obvykle, pokud bude jasné, ve které grupě počítáme, budeme psát pouze 1 místo 1_G, operace násobení nebudeme rozlišovat různými symboly a někdy budeme místo $g \cdot h$ a $A \cdot B$ psát pouze gh a AB.

Věta 2.18 (jádro a obraz homomorfismu) *Ať je $f : G \to \overline{G}$ homomorfismus grup. Pak je $\mathrm{Im}(f)$ podgrupa $\overline{G}$ a $\mathrm{Ker}(f)$ je normální podgrupa G. Přitom jsou grupy $\mathrm{Im}(f)$ a $G/\mathrm{Ker}(f)$ izomorfní.*

Důkaz. Homomorfismy grup zachovávají násobení, neutrální i inverzní prvky, tedy $\mathrm{Im}(f)$ je podgrupa $\overline{G}$. Položme $g \sim_f h$ pro $g, h \in G$, pokud $f(g) = f(h)$. Relace $\sim_f$ je jistě ekvivalence na G. Pro $g_1, g_2, h_1, h_2 \in G$, $f(g_1) = f(g_2)$ a $f(h_1) = f(h_2)$, máme $f(g_1h_1) = f(g_1)f(h_1) = f(g_2)f(h_2) = f(g_2h_2)$. Relace $\sim_f$ je kongruence na G a $[1]_{\sim_f} = \mathrm{Ker}(f)$ je tudíž normální podgrupa G.

Označme $K = \mathrm{Ker}(f)$. Podle předchozího odstavce je $\sim_f$ kongruence, $[1]_{\sim_f} = K$ a tedy jsou třídy $\sim_f$ totožné s rozkladovými třídami podle K. Z toho plyne, že zobrazení $\varphi : G/K \to \mathrm{Im}(f)$, definované předpisem $\varphi(gK) = f(g)$, je dobře definovaná bijekce. Zbývá ukázat vlastnost homomorfismu: $\varphi(gK \cdot hK) = \varphi(gKhK) = \varphi(ghKK) = \varphi(ghK) = f(gh) = f(g)f(h) = \varphi(gK) \cdot \varphi(hK)$. □

Podle předchozího tedy máme tento vztah:

Kongruence odpovídají přesně normálním podgrupám a také jádrům homomorfismů.

Příklady. 1) Mějme $C = (i_0 i_1 ... i_{l-1}) \in \mathrm{S}_n$ cyklus délky l. Snadno se spočítá, že je $C = (i_0 i_{l-1}) \circ (i_0 i_{l-2}) \circ ... \circ (i_0 i_3) \circ (i_0 i_2) \circ (i_0 i_1)$ složení cyklů délky 2 (skládáme zprava). Cykly délky 2 se nazývají *transpozice*. Každá permutace je složení (nezávislých) cyklů, tedy každá permutace lze zapsat jako složení transpozic. Je-li $\pi = T_1 \circ T_2 \circ ... \circ T_r$, T_i transpozice pro $i = 1, ..., r$, pak definujeme znaménko $\mathrm{sgn}(\pi) = (-1)^r$. Zopakujte si, že je tato definice korektní (Hint: Uspořádaná dvojice (i, j), $1 \le i, j \le n$, se nazývá *inverze* v permutaci π, pokud $i < j$ a $\pi(i) > \pi(j)$. Ukažte, že se počet inverzí dané permutace, složíme-li ji s transpozicí, změní o liché číslo. Takto lze ukázat, že $\mathrm{sgn}(\pi) = (-1)^q$, kde q je počet inverzí v π. Z toho plyne, že definice znaménka nezávisí na volbě zápisu π jako složení transpozic.)

Znaménko je homomorfismus $\mathrm{S}_n \to \{1, -1\}$, kde na množině $\{1, -1\}$ máme operaci násobení celých čísel (uvědomte si, že $\{1, -1\} \cong \mathbb{Z}_2$). Totiž $\mathrm{sgn}(\pi \circ \psi) = \mathrm{sgn}(T_1 \circ T_2 \circ ... \circ T_r \circ T'_1 \circ T'_2 \circ ... \circ T'_s) = (-1)^{r+s} = (-1)^r(-1)^s = \mathrm{sgn}(\pi) \cdot \mathrm{sgn}(\psi)$, kde $\pi = T_1 \circ T_2 \circ ... \circ T_r$ a $\psi = T'_1 \circ T'_2 \circ ... \circ T'_s$ jsou složení transpozic. Normální podgrupa $\mathrm{Ker}(\mathrm{sgn})$ se nazývá *alternující grupa* a značí se A_n. Prvky A_n se nazývají *sudé* permutace, prvky $\mathrm{S}_n \setminus \mathrm{A}_n$ jsou *liché* permutace. Podle Věty 2.18 je $\mathrm{S}_n/\mathrm{A}_n \cong \{1, -1\}(\cdot) \cong \mathbb{Z}_2$ pro $n > 1$.

2) Jak víte, determinant je homomorfismus z pologrupy všech matic řádu n nad tělesem T s operací násobení matic, značíme ji $\mathrm{M}_n(T)$, do pologrupy $T(\cdot)$ násobení skalárů v tělese. Označme $\mathrm{GL}_n(T)$ grupu všech regulárních matic řádu n nad T. Tato grupa se obvykle nazývá *obecná lineární grupa* (general linear group). Zúžení determinantu na $\mathrm{GL}_n(T)$ je homomorfismus grup, $\det : \mathrm{GL}_n(T) \to (T \setminus \{0\})(\cdot)$. Jádro $\mathrm{Ker}(\det)$ se nazývá *speciální lineární grupa* (special linear group) a značí se $\mathrm{SL}_n(T)$. Podle Věty 2.18 je $\mathrm{GL}_n(T)/\mathrm{SL}_n(T) \cong (T \setminus \{0\})(\cdot)$.

Úkol. Pro S a $\overline{S}$ pologrupy víme, že potence $\mathrm{P}(S)$ a $\mathrm{P}(\overline{S})$ jsou s indukovaným násobením opět pologrupy. Ukažte, že homomorfismus $f : S \to \overline{S}$ indukuje homomorfismus $\mathrm{P}(S) \to \mathrm{P}(\overline{S})$, kde $A \mapsto f(A)$.

Věta 2.19 *Ať je $f : G \to \overline{G}$ epimorfismus grup. Pak je přiřazení $\overline{H} \mapsto f^{-1}(\overline{H})$ bijekce z množiny normálních podgrup $\overline{G}$ na množinu normálních podgrup G obsahujících* $\mathrm{Ker}(f)$.

Důkaz. Pro $\overline{H}$ podgrupu $\overline{G}$ je úplný vzor $H = f^{-1}(\overline{H})$ podgrupa G. Totiž pro $g, h \in H$ je $f(g), f(h) \in \overline{H}$ a máme $f(gh) = f(g)f(h) \in \overline{H}$. Tedy H je uzavřená na násobení a podobně lze ukázat uzavřenost na neutrální a inverzní prvky. Dále je $\mathrm{Ker}(f) \leq H$, neboť $1 \in \overline{H}$.

Označme $K = \mathrm{Ker}(f)$ a předpokládejme, že $\overline{H} \lhd \overline{G}$. Zvolme $g \in G$. Platí $f(g)\overline{H} = \overline{H}f(g)$ a tedy $f^{-1}(f(g)\overline{H}) = f^{-1}(\overline{H}f(g))$. Jistě platí $gH \subseteq f^{-1}(f(g)\overline{H})$. Naopak pro $g' \in f^{-1}(f(g)\overline{H})$ existuje $h \in H$ tak že $f(g') = f(g)f(h) = f(gh)$ a tedy $g' \in ghK$ podle Věty 2.18. Dostáváme $g' \in gH$, neboť $hK \subseteq H$, a $f^{-1}(f(g)\overline{H}) \subseteq gH$. Dokázali jsme rovnost $gH = f^{-1}(f(g)\overline{H})$ a obdobně se dokáže, s použitím $hgK = Khg$, rovnost $Hg = f^{-1}(\overline{H}f(g))$. Tudíž $gH = Hg$ a $H \lhd G$.

Přiřazení ze znění věty je tedy na daných množinách dobře definované. Dosud jsme nepoužili, že f je epimorfismus. Mějme $\overline{H_1}$ a $\overline{H_2}$ dvě normální podgrupy $\overline{G}$, $\overline{H_1} \neq \overline{H_2}$. Ať například existuje $\overline{h} \in \overline{H_1} \setminus \overline{H_2}$. Pak pro $h \in G$ takové, že $f(h) = \overline{h}$ (f je epimorfismus), platí $h \in H_1 \setminus H_2$, kde $H_1 = f^{-1}(\overline{H_1})$ a $H_2 = f^{-1}(\overline{H_2})$. Tedy $H_1 \neq H_2$ a přiřazení ze znění věty je prosté.

Zvolme $H \lhd G$, $K = \mathrm{Ker}(f) \leq H$. Podle Věty 2.18 pro $g \in G$ platí $f^{-1}(f(g)) = gK$. Dále jistě platí $H = \bigcup_{h \in H} hK$ a tak dostáváme $H = \bigcup_{h \in H} f^{-1}(f(h)) = f^{-1}(f(H))$. Položme $\overline{H} = f(H)$. Máme $f^{-1}(\overline{H}) = H$. Pokud ukážeme, že je $\overline{H} \lhd \overline{G}$, bude zkoumané přiřazení také na. Uvážíme-li restrikci f na H, dostaneme homomorfismus $H \to \overline{G}$ a tedy podle Věty 2.18 je $\overline{H}$ podgrupa $\overline{G}$. Pro $\overline{g} \in \overline{G}$ zvolme $g \in G$ tak, že $\overline{g} = f(g)$ (opět používáme, že f je epimorfismus). Platí $gH = Hg$, $f(gH) = f(g)f(H) = \overline{g}\overline{H}$ a také $f(Hg) = \overline{H}\overline{g}$, tedy $\overline{g}\overline{H} = \overline{H}\overline{g}$ a $\overline{H} \lhd \overline{G}$. □

Věta 2.20 (věta o izomorfismu) *Je-li $f : G \to \overline{G}$ epimorfismus grup a $\overline{H} \lhd \overline{G}$, pak jsou grupy $\overline{G}/\overline{H}$ a $G/f^{-1}(\overline{H})$ izomorfní.*

Důkaz. Podle Věty 2.19 je $H = f^{-1}(\overline{H})$ normální podgrupa G a tedy můžeme uvažovat faktor G/H. Označme $p : \overline{G} \to \overline{G}/\overline{H}$ přirozenou projekci a označme $\tilde{f} = p \circ f : G \to \overline{G}/\overline{H}$ (skládáme zprava). Oba homomorfismy f i p jsou epimorfismy, tedy jejich složení

$\tilde{f}$ je opět epimorfismus. Pro $g \in G$ platí $g \in \mathrm{Ker}(\tilde{f})$ právě když $f(g) \in \mathrm{Ker}(p)$. Tedy $g \in \mathrm{Ker}(\tilde{f})$ právě když $f(g) \in \overline{H}$, což je právě když $g \in H$. Zjistili jsme, že $H = \mathrm{Ker}(\tilde{f})$ a to podle Věty 2.18 znamená, že $G/H \cong \mathrm{Im}(\tilde{f}) = \overline{G}/\overline{H}$. □

Definice. Grupa G se nazývá jednoduchá, pokud jsou 1 a G jediné normální podgrupy G (zde 1 značí takzvanou triviální podgrupu, přesněji zapsáno $\{1\}$).

Příklad. Ať je G grupa, $|G| = p$. Je-li p prvočíslo, pak je G jednoduchá a izomorfní $\mathbb{Z}_p$. Totiž podle Lagrangeovy věty musí být 1 a G dokonce jediné podgrupy G, neboť 1 a p jsou jediní dělitelé p. Zvolme $g \in G$, $g \neq 1$. Platí $|\langle g \rangle| \geq 2$ a tedy ze stejného důvodu musí být $\langle g \rangle = G$. Podle Lemmatu 2.8 je $G \cong \mathbb{Z}_p$.

Definice. Prvky h, k grupy G se nazývají *konjugované* pokud existuje $g \in G$ tak, že $ghg^{-1} = k$.

Úkol. Ukažte, že relace "být konjugované" je ekvivalence na grupě G.

Příklad. Porovnáním definic snadno zjistíte, že dvě matice $A, B \in \mathrm{GL}_n(T)$ jsou konjugované právě když jsou podobné.

Poznámka. Snadno se ukáže, že

podgrupa H grupy G je normální právě když je uzavřená na konjugované prvky,

tedy jsou-li $h \in H$ a $k \in G$ konjugované, pak je $k \in H$. Totiž pro $g \in G$ platí $gH = Hg$, tedy $H = gHg^{-1}$ a proto je $ghg^{-1} \in H$ pro každé $h \in H$. Naopak je-li H uzavřená na konjugované prvky, pak $gh = ghg^{-1}g = (ghg^{-1})g = h'g$, tedy $gH \subseteq Hg$, a také $hg = gg^{-1}hg = g(g^{-1}hg) = gh'$ (uvědomte si, že $g^{-1}hg$ je také zápis konjugovaného prvku pro $g \mapsto g^{-1}$), tedy $Hg \subseteq gH$.

Lemma 2.21 *Dvě permutace z S_n jsou konjugované právě když mají stejný typ.*

Důkaz. Mějme $\pi, \gamma \in \mathrm{S}_n$. Pro konjugovaný prvek $\gamma\pi\gamma^{-1}$ (připomeňme, že skládáme zprava) platí:

$$\gamma(i) \overset{\gamma^{-1}}{\longmapsto} i \overset{\pi}{\longmapsto} \pi(i) \overset{\gamma}{\longmapsto} \gamma(\pi(i)).$$

Pro $C = (i_0 i_1 ... i_{l-1})$ cyklus délky l platí $C(i_j) = i_{(j+1 \bmod l)}$, tedy $(\gamma C \gamma^{-1})(\gamma(i_j)) = \gamma(i_{(j+1 \bmod l)})$ a permutace $\gamma C \gamma^{-1} = (\gamma(i_0)\gamma(i_1)...\gamma(i_{l-1}))$ je opět cyklus délky l.

Je-li $\pi = C_1 C_2 ... C_r$ rozklad π na nezávislé cykly, pak $\gamma\pi\gamma^{-1} = \gamma C_1 C_2 ... C_r \gamma^{-1} = \gamma C_1 \gamma^{-1} \gamma C_2 \gamma^{-1} \gamma ... \gamma^{-1} \gamma C_r \gamma^{-1}$ a π je tedy složení cyklů $\gamma C_k \gamma^{-1}$, $k = 1, ..., r$. Z předchozího odstavce a z toho, že γ je permutace plyne, že jsou cykly $\gamma C_k \gamma^{-1}$ nezávislé. Tedy konjugované permutace mají stejný typ.

Naopak předpokládejme, že permutace π a ψ mají stejný typ. Ať jsou $\pi = C_1 C_2 ... C_r$ a $\psi = C'_1 C'_2 ... C'_r$ rozklady na nezávislé cykly takové, že cykly C_k a C'_k mají stejnou délku l_k pro $1 \leq k \leq r$. Označme $C_k = (i_{k0} i_{k1} ... i_{k(l_k-1)})$ a $C'_k = (i'_{k0} i'_{k1} ... i'_{k(l_k-1)})$. Definujme zobrazení γ takto: $\gamma(i_{kj}) = i'_{kj}$ pro $1 \leq k \leq r$ a $0 \leq j \leq l_k - 1$. Z nezávislosti cyklů C_k

a cyklů C'_k plyne, že γ je dobře definovaná permutace, a z první části důkazu vidíme, že $\gamma\pi\gamma^{-1} = \psi$. □

Z Lemmatu a Poznámky přímo plyne:

Důsledek 2.22 *Podgrupa grupy* S_n *je normální právě když s každou svou permutací obsahuje všechny permutace stejného typu.*

Příklad. Označme $K_4 = \{(12)(34), (13)(24), (14)(23), 1\} \subseteq S_4$. Snadno se ukáže, že K_4 je podgrupa S_4 (je to vlastně podgrupa A_4). Neutrální prvek leží v K_4 a pro všechna $\pi \in K_4$ platí $\pi^2 = 1$ a tedy $\pi^{-1} = \pi \in K_4$. Složíme-li dvě různé neidentické permutace z K_4, dostaneme třetí neidentickou permutaci. Například $(12)(34) \circ (13)(24) = (14)(23) = (13)(24) \circ (12)(34)$. Vidíme, že je K_4 komutativní grupa. Dále K_4 obsahuje 1 a všechny permutace typu $[2, 2]$, tedy je podle Důsledku 2.22 normální v S_4 (a tedy i v A_4). Grupa K_4 se nazývá *Kleinova 4-grupa.*

Věta 2.23 *Grupa* A_n *je jednoduchá právě když je* $n \neq 4$.

Důkaz. Pro $n = 1, 2$ obsahuje A_n pouze neutrální prvek. Dále je $A_3 = \{(123), (321), 1\} = \langle(123)\rangle$, tedy A_3 je jednoduchá grupa izomorfní $\mathbb{Z}_3$.

Pro $n = 4$ je Kleinova 4-grupa normální v A_4, tedy A_4 není jednoduchá.

Zbytek důkazu rozdělíme do několika kroků.

1. krok. Trojcykly generují A_n.
Víme, že množina všech transpozic je množinou generátorů grupy S_n pro každé $n \in \mathbb{N}$. Nyní ukážeme, že množina všech cyklů délky 3 (tedy *trojcyklů*) generuje A_n pro každé $n \in \mathbb{N}$. Snadno si ověříte, že pokud se transpozice překrývají právě v jednom čísle, pak je jejich složení trojcyklus, a že pro nezávislé transpozice $T = (ij)$ a $T' = (i'j')$ platí $T'T = (i'ij')(iji')$. Sudá permutace π má rozklad na součin transpozic $\pi = T_1T_2...T_{2r}$ pro vhodné $r \in \mathbb{N} \cup \{0\}$. Ať je r nejmenší možné. Pak pro $1 \leq i \leq r$ jsou transpozice T_{2i-1}, T_{2i} buď nezávislé, nebo se překrývají v jednom čísle, a v obou těchto případech lze jejich složení vyjádřit jako složení trojcyklů.

Ať je pro zbytek důkazu $n \geq 5$.

2. krok. Trojcykly jsou konjugované v A_n *pro* $n \geq 5$.
Víme, že všechny trojcykly jsou v S_n konjugované. Pro trojcykly $C, C' \in S_n$ tedy existuje $\gamma \in S_n$ tak, že $\gamma C\gamma^{-1} = C'$. Je-li γ sudá, pak jsou C a C' konjugované v A_n. Je-li γ lichá, zvolme transpozici T tak, aby T a C' byly nezávislé. Máme $C' = C'TT^{-1} = C'TT = TC'T = T\gamma C\gamma^{-1}T = (T\gamma)C(\gamma^{-1}T^{-1}) = (T\gamma)C(T\gamma)^{-1}$, kde $T\gamma$ je sudá permutace. Dokázali jsme, že pro $n \geq 5$ jsou všechny trojcykly konjugované v A_n. Pokud normální podgrupa $H \triangleleft A_n$ obsahuje nějaký trojcyklus, pak obsahuje všechny trojcykly, tedy množinu generátorů A_n, a proto musí být $H = A_n$.

3.krok. Pro $n \geq 5$ *obsahuje netriviální normální podgrupa* A_n *trojcyklus.*
Mějme $H \triangleleft A_n$, $H \neq 1$ (přesněji $H \neq \{1\}$). Pro $\pi \in S_n$ a $1 \leq i \leq n$ řekneme, že i je pevný bod π, pokud $\pi(i) = i$. Zvolme $1 \neq \pi \in H$ s největším počtem pevných

bodů. Ukážeme, že π musí být trojcyklus. Ať je $\pi = C_1C_2...C_r$, kde C_k, $k = 1, ..., r$, jsou nezávislé cykly délky alespoň 2.

Ať je délka některého z cyklů, například C_1, alespoň 3. Buď je $r = 1$ a π je trojcyklus, což jsme chtěli ukázat, nebo alespoň čtyři čísla nejsou pevné body π. Položme $C_1 = (i_0 i_1 i_2\ ...)$ a zvolme $1 \leq i \leq n$ různé od i_0, i_1, i_2, které není pevný bod π. Položme $\gamma = (i_0 i i_2)$. Každý pevný bod π je pevným bodem γ i $\gamma^{-1} = (i_2 i i_0)$. Z toho plyne, že pevné body π jsou i pevnými body permutace $\psi = \gamma\pi\gamma^{-1} \in H$ a tedy i složení $\psi\pi \in H$. V rozkladu ψ na nezávislé cykly bude cyklus

$$\gamma C_1 \gamma^{-1} = (\gamma(i_0)\gamma(i_1)\gamma(i_2)\ ...) = (i i_1 i_0\ ...),$$

tedy $\psi(i_1) = i_0$, a pro složení dostáváme $\psi\pi(i_0) = i_0$. Tudíž $\psi\pi$ má více pevných bodů než π. Zároveň $\psi\pi(i_1) \neq i_1$, neboť $\pi(i_1) = i_2$ a $\psi(i_2) \neq i_1$, protože $\psi(i) = i_1$. Tedy $\psi\pi \neq 1$ a to je spor.

Zbývá případ, že všechny cykly C_k, $k = 1, ..., r$, jsou transpozice. Ať je $r > 2$. Označme $C_1 = (ij)$, $C_2 = (i'j')$, a položme $\gamma = (ii') \circ C_3$. Konjugováním získáme $\psi = \gamma\pi\gamma^{-1} = (i'j)(ij')C_3^3C_4...C_r$ a tedy

$$\psi = (i'j)(ij')C_3C_4...C_r \in H.$$

Složením dostaneme $\psi\pi = (i'j)(ij') \circ (ij)(i'j') = (ii')(jj') \in H$ (podle skládání v Kleinově 4-grupě). Opět jsme zvětšili počet pevných bodů, což je spor. Vidíme, že $\pi = C_1C_2 = (ij)(i'j')$. Vyberme $1 \leq l \leq n$ číslo různé od všech i, j, i', j' (to lze pro $n \geq 5$) a položme $\gamma = (lj)(i'j')$. Platí $\delta = \gamma\pi\gamma^{-1} = (il)(j'i') = (il)(i'j') \in H$ a pro složení:

$$\delta\pi = (ijl) \in H.$$

Permutace $\delta\pi$ má o jeden pevný bod více, což je spor.

Dokázali jsme, že π je trojcyklus. Tedy H obsahuje trojcyklus a tudíž je $H = \mathrm{A}_n$. Vidíme, že A_n je pro $n \geq 5$ jednoduchá grupa. □

Lemma 2.24 *Pro K podgrupu grupy G a $H \lhd G$ platí: $H \cap K \lhd K$, $KH = HK$ je podgrupa generovaná sjednocením $H \cup K$ a $KH/H \cong K/(H \cap K)$.*

Důkaz. Buď $p : G \to G/H$ přirozená projekce a označme $p' : K \to G/H$ restrikci p na K. Víme, že $\mathrm{Ker}(p) = H$ a tedy $\mathrm{Ker}(p') = H \cap K$. Podle Věty 2.18 je $H \cap K \lhd K$. Platí $H \cup K \subseteq KH = HK$ neboť $1 \in K$, $1 \in H$ a H je normální a naopak množina KH musí být obsažena v každé podgrupě G, která obsahuje $H \cup K$. Z počítání ve faktoru víme, že $(k_1H) \cdot (k_2H) = k_1k_2H$, tedy pro $k_1, k_2 \in K$ a $h_1, h_2 \in H$ platí $(k_1h_1) \cdot (k_2h_2) \in k_1k_2H \subseteq KH$ a vidíme, že je množina KH uzavřená na násobení. Dále je $1 \in H \cap K$ a tudíž $1 \in KH$ a pro inverze platí $(kh)^{-1} = h^{-1}k^{-1} \in HK = KH$. Ukázali jsme, že je KH podgrupa G generovaná $H \cup K$.

Označme $\overline{K} = \mathrm{Im}(p')$. Zvolme $k \in K$ a $h \in H$. Platí $p(kh) = p(k)p(h) = p(k) \cdot 1 = p(k)$, tedy $p(KH) = p(K) = \overline{K}$. Můžeme tedy uvážit $p'' : KH \to \overline{K}$ restrikci p, což je epimorfismus grup, pro který platí $\mathrm{Ker}(p'') = H \cap KH = H$. Podle Věty 2.18 je $KH/H \cong \overline{K}$ a zároveň podle stejné Věty, uvážíme-li restrikci p', je $K/(H \cap K) \cong \overline{K}$. Tedy $KH/H \cong K/(H \cap K)$. □

Definice. Posloupnost $H_0 \leq H_1 \leq ... \leq H_{n-1} \leq H_n$ podgrup grupy G se nazývá *subnormální řada*, pokud pro všechna $i = 0, ..., n-1$ platí $H_i \lhd H_{i+1}$. Faktory H_{i+1}/H_i se nazývají *vrstvy* subnormální řady.

Pozor: Pojem normální podgrupy (na rozdíl od podgrupy) není tranzitivní: je-li $H \lhd K$ a zároveň $K \lhd G$, pak H nemusí být normální v G. Příklad lze nalézt v S_4. Položme $H = \{(12) \circ (34),\ 1\}$, $K =$ K_4 Kleinova 4-grupa a $G =$ S_4. Grupa K je komutativní a tedy všechny její podgrupy jsou normální, proto $H \lhd K$. Dále je $K \lhd G$, neboť obsahuje všechny permutace typu $[2, 2]$, ale ze stejného důvodu není H normální v G (K je nejmenší normální podgrupa G obsahující H).

Následující tvrzení je podstatné pro práci se subnormálními řadami.

Lemma 2.25 *Ať je $H_0 \lhd H_1 \lhd ... \lhd H_{n-1} \lhd H_n$ subnormální řada v grupě G.*

1) Je-li K podgrupa G, pak je $H_0 \cap K \lhd H_1 \cap K \lhd ... \lhd H_{n-1} \cap K \lhd H_n \cap K$ subnormální řada. Navíc existují přirozené monomorfismy $H_{i+1} \cap K \,/\, H_i \cap K \to H_{i+1}/H_i$ pro $i = 0, ..., n-1$, tedy vrstvy nové řady můžeme chápat jako podgrupy vrstev původní řady.

2) Je-li K normální podgrupa G, pak je $H_0K \lhd H_1K \lhd ... \lhd H_{n-1}K \lhd H_nK$ subnormální řada. Navíc existují přirozené epimorfismy $H_{i+1}/H_i \to H_{i+1}K/H_iK$ pro $i = 0, ..., n-1$, tedy vrstvy nové řady můžeme chápat jako faktory vrstev původní řady.

Důkaz. 1) Položme $K_i = H_i \cap K$ pro $i = 0, ..., n$. Pro $0 \leq i \leq n-1$ je $H_i \lhd H_{i+1}$ a K_{i+1} je podgrupa H_{i+1}, tedy podle Lemmatu 2.24 je $K_i = H_i \cap K = H_i \cap H_{i+1} \cap K = H_i \cap K_{i+1} \lhd K_{i+1}$. Dále, opět podle Lemmatu 2.24, je $K_{i+1}/K_i = K_{i+1}/\ H_i \cap K_{i+1} \cong K_{i+1}H_i/H_i \leq H_{i+1}/H_i$.

2) Položme $K_i = H_iK$ pro $i = 0, ..., n$. Podle Lemmatu 2.24 jsou K_i podgrupy G. Zvolme $g = hk \in K_{i+1}$, $h \in H_{i+1}$ a $k \in K$. Máme $gK_i = hkH_iK = hkKH_i = hKH_i = hH_iK = H_ihK = H_ihKk = H_iKhk = K_ig$, tedy $K_i \lhd K_{i+1}$. Pro vrstvy platí:

$$K_{i+1}/K_i = H_{i+1}K/H_iK = (H_{i+1}H_i)K/H_iK =$$
$$= H_{i+1}(H_iK)/H_iK \cong H_{i+1}/\ (H_iK) \cap H_{i+1}.$$

Označme $D_i = (H_iK) \cap H_{i+1}$. Jistě je $H_i \leq D_i$ a tedy podle Vět 2.19 a 2.20 existuje přirozený epimorfismus $H_{i+1}/H_i \to H_{i+1}/D_i \cong K_{i+1}/K_i$. □

Grupa se nazývá *komutativní*, pokud pro každé dva její prvky g a h platí $g \cdot h = h \cdot g$. Nyní budeme definovat širší třídu grup, která se dá chápat jako zobecnění komutativních grup.

Definice. Grupa G se nazývá *řešitelná*, pokud existuje subnormální řada $1 = H_0 \lhd H_1 \lhd ... \lhd H_{n-1} \lhd H_n = G$ taková, že všechny její vrstvy jsou komutativní. Je-li n nejmenší, pro které taková řada existuje, pak se G nazývá řešitelná grupa *stupně* n.

Vidíme, že grupa je komutativní, neboli *abelovská*, právě když je řešitelná stupně 0 nebo 1. Řešitelné grupy stupně 2 se někdy nazývají *meta-abelovské*.

Věta 2.26 *Faktor i podgrupa řešitelné grupy stupně nejvýše n je opět řešitelná grupa stupně nejvýše n.*

Důkaz. Tvrzení jistě platí pro komutativní grupy. Podgrupa komutativní grupy je opět komutativní a je-li $f : G \to \overline{G}$ epimorfismus grup, kde G je komutativní, pak pro $\overline{g}, \overline{h} \in \overline{G}$ zvolíme vzory $g, h \in G$, $f(g) = \overline{g}$ a $f(h) = \overline{h}$, a máme: $\overline{g} \cdot \overline{h} = f(g) \cdot f(h) = f(g \cdot h) = f(h \cdot g) = f(h) \cdot f(g) = \overline{h} \cdot \overline{g}$.

Ať je nyní G řešitelná grupa a $1 = H_0 \lhd H_1 \lhd ... \lhd H_{n-1} \lhd H_n = G$ ať je subnormální řada s komutativními vrstvami.

Pro K podgrupu G položme $K_i = H_i \cap K$ pro $i = 0, ..., n$. Podle Lemmatu 2.25 je $K_0 \lhd K_1 \lhd ... \lhd K_{n-1} \lhd K_n$ subnormální řada s komutativními vrstvami a přitom je jistě $K_0 = 1$ a $K_n = K$.

Buď $f : G \to \overline{G}$ epimorfismus. Označme $K = \mathrm{Ker}(f)$. Položme $K_i = H_i K$, $i = 0, ..., n$. Podle Lemmatu 2.25 je $K_0 \lhd K_1 \lhd ... \lhd K_{n-1} \lhd K_n$ subnormální řada s komutativními vrstvami. Je zřejmé, že $K_0 = K$ a $K_n = G$. Na závěr položme $\overline{K_i} = f(K_i)$. Uvážíme-li restrikci f na podgrupu K_{i+1}, pak podle Věty 2.19 je $K_i = f^{-1}(\overline{K_i})$, $\overline{K_i} \lhd \overline{K_{i+1}}$ a podle Věty 2.20 platí: $\overline{K_{i+1}}/\overline{K_i} \cong K_{i+1}/K_i$. Tedy $1 = \overline{K_0} \lhd \overline{K_1} \lhd ... \lhd \overline{K_{n-1}} \lhd \overline{K_n} = \overline{G}$ je opět subnormální řada s komutativními vrstvami. □

Věta 2.27 *Grupa S_n je řešitelná právě když je $n \leq 4$.*

Důkaz. Pro $n = 1$ nebo $n = 2$ je S_n komutativní. Pro $n = 3$ je A_3 tříprvková grupa, tedy $\mathrm{A}_3 \cong \mathbb{Z}_3$ je komutativní. Dále $\mathrm{S}_n/A_n \cong \mathbb{Z}_2$ (pro $n > 1$) a subnormální řada $1 \lhd \mathrm{A}_3 \lhd \mathrm{S}_3$ má komutativní vrstvy.

Pro $n = 4$ má subnormální řada $1 \lhd \mathrm{K}_4 \lhd \mathrm{A}_4 \lhd \mathrm{S}_4$ faktory $\mathrm{K}_4/1 \cong \mathrm{K}_4$, $\mathrm{A}_4/\mathrm{K}_4$ je podle Věty 2.6 tříprvková grupa a tedy $\mathrm{A}_4/\mathrm{K}_4 \cong \mathbb{Z}_3$ a konečně $\mathrm{S}_4/\mathrm{A}_4 \cong \mathbb{Z}_2$. Všechny faktory jsou komutativní.

Je-li $n \geq 5$, pak je podle Věty 2.23 grupa A_n jednoduchá. Pokud by A_n byla řešitelná, pak by musela být komutativní. Víme ale například, že všechny trojcykly jsou v A_n pro $n \geq 5$ konjugované, tedy A_n nemůže být komutativní. Tudíž pro $n \geq 5$ není A_n řešitelná a podle Věty 2.26 není ani S_n řešitelná. □

Poznámka. Subnormální řada $1 = H_0 \lhd H_1 \lhd ... \lhd H_n = G$ se nazývá *kompoziční řada*, pokud jsou všechny její vrstvy netriviální jednoduché grupy. V netriviální konečné grupě vždy existují v inkluzi maximální normální podgrupy, tedy podgrupy $H \lhd G$ takové, že $H \neq G$ a kdykoli $H \leq K \lhd G$, pak $K = H$ nebo $K = G$. Podle Věty 2.19 je pro maximální $H \lhd G$ faktor G/H jednoduchá grupa. Tedy v konečné grupě lze vždy indukcí zkonstruovat kompoziční řadu. Pro kompoziční řady platí následující tvrzení, které zde nebudeme dokazovat.

Věta (Jordan–Hölderova věta) *Jsou-li $1 = H_0 \lhd H_1 \lhd ... \lhd H_n = G$ a $1 = K_0 \lhd K_1 \lhd ... \lhd K_m = G$ dvě kompoziční řady, pak $n = m$ a obě řady mají, až na pořadí, izomorfní vrstvy. Jinými slovy existuje permutace $\pi \in S_n$ tak, že $H_i/H_{i-1} \cong K_{\pi(i)}/K_{\pi(i)-1}$ pro všechna $1 \leq i \leq n$.*