Grupy a reprezentace 4

Zpracováno na základě poznámek J. Mareše a s jejich využitím

wiki-skripta

Prostá grupa

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 $x^n = \left(x^k\right)^{\frac{n}{k}} = e$. Protože p dělí n, tj. $n = pk$, platí $x^n = x^{kp} = \left(x^k\right)^p = e$, tj. x^k má řád p. $\square$

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

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

!! Součin podgrup nemusí být podgrupou!!

Theorem

Nechť H a K jsou podgrupy konečné grupy G, pak

$$|HK| = \frac{|H||K|}{|H \cap K|}. \tag{1}$$

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

$$HK = K \cup h_1 K \cup \ldots h_s K$$

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

Důkaz.

HK můžeme napsat jako sjednocení levých tříd K,

$$HK = \bigcup_{h \in H} hK. \tag{2}$$

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

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

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 má $|K|$ prvků, čímž dostáváme tvrzení věty. $\square$

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

$$ab^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = h_1 k_3 h_2^{-1} \tag{4}$$

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

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

□

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

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

□

Corollary

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

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

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 $\varphi : G \to H$ *je homomorfismus, pak* $Ker\ \varphi \trianglelefteq G$ *a* $G/Ker\ \varphi \cong \varphi(G)$.

Důkaz.

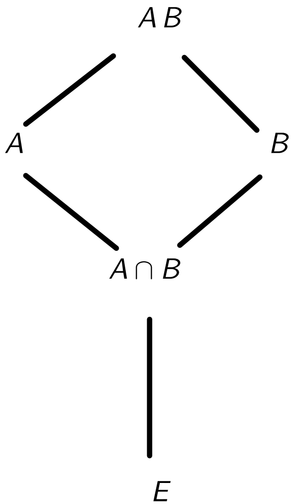
První část je zřejmá z předchozích vět. Důkaz druhé spočívá v ověření, že $\varphi' : G/Ker\ \varphi \to \varphi(G) : \varphi'(gKer\ \varphi) = \varphi(g)$ *je izomorfismus, což je plyne z definic a předchozího.* $\square$

Corollary

Buď $\varphi : G \to H$ *homomorfismus. Potom platí:*

1. φ *je izomorfismus* $\Leftrightarrow Ker\ \varphi = e_G$,
2. $|G : Ker\ \varphi| = |\varphi(G)|$.

2. Věta o isomorfismu - diamantová



Theorem (2. VOI, „diamantová“)

Buď 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 $AB/B \cong A/A \cap B$.

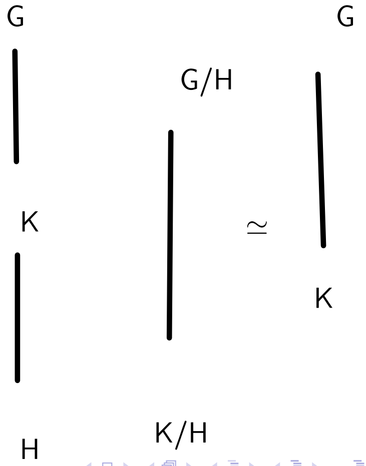
Důkaz.

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 $\varphi : A \to AB/B$ předpisem $\varphi(a) = aB$:

$$\varphi(a_1 a_2) = (a_1 a_2)B = a_1 B a_2 B = \varphi(a_1)\varphi(a_2). \tag{8}$$

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 $A/A \cap B \cong AB/B$. $\square$

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



Theorem (3. VOI)

Buď 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 $K/H \trianglelefteq G/H$:

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

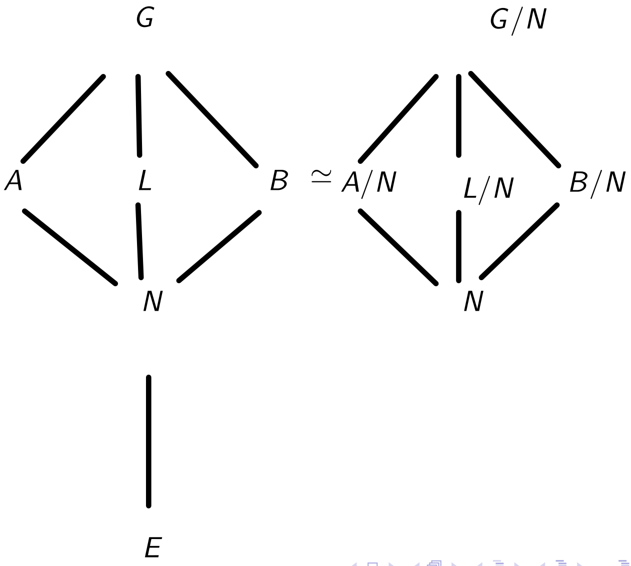
Definujeme homomorfismus $\varphi : G/H \to G/K$ předpisem $\varphi(gH) = gK$. Abychom ukázali že φ je dobře definované, vezmeme $g_1H = g_2H$. Potom $g_1 = g_2h$ pro nějaké $h \in H$. Protože $H \leq K$, je taky $h \in K$, proto $g_1K = g_2K$. Tudíž $\varphi(g_1H) = \varphi(g_2H)$ a φ je dobře definované.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

$$\operatorname{Ker} \varphi = \{gH \in G/H | \varphi(gH) = K\} = \{gH \in G/H | gK = K\} = \tag{10}$$

$$= \{gH \in G/H | g \in K\} = K/H, \tag{11}$$

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

4. Věta o isomorfismu - o grafech faktor grup



Následují 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“] Buď 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

1. $B \leq A \Leftrightarrow B/N \leq A/N$,
2. *Je–li* $A \leq B$, *pak* $|B : A| = |B/N : A/N|$,
3. $< A, B > /N =< A/N, B/N >$,
4. $A/N \cap B/N = (A \cap B)/N$,
5. $A \trianglelefteq G \Leftrightarrow A/N \trianglelefteq G/N$.

Důkaz 1) a 2)

Ověříme, že zobrazení θ definované pomocí $A \mapsto A/N$ je bijekce: Nejprve prostota. Nechť $A/N = B/N$. Pak $\forall a \in A$ platí $aN = bN$ pro nějaké $b \in B$, tj. $a^{-1}b \in N \subset B$. Proto $a \in B$ a $A \subset B$. Druhá inkluze se dokáže stejně.
Nyní surjektivita: Je–li S podgrupa G/N, a $\phi : G \to G/N$, pak $\phi^{-1}(S) = \{s \in G | sN \in S\}$ je podgrupa G (platí $uNvN = uvN$) obsahující $N = \phi^{-1}(\{e\})$ a $\theta(\phi^{-1}(S)) = \{sN | sN \in S\} = S$, což dokazuje surjektivitu.
Nyní ověříme vlastnosti:

1) Z $A \leq B$ plyne $A/N \leq B/N$ díky tomu, že operace na levých třídách je díky $N \trianglelefteq G$ dobře definovaná, obráceně proto, že θ je bijekce.
2) Zobrazení ψ zobrazuje levé třídy v B/A do levých tříd v $(B/N)/(A/N)$ tak, že pro $b \in B$ zobrazí bA na $(bN)(A/N)$. ψ je dobře definované a prosté, protože $b_1 A = b_2 A \Leftrightarrow b_1^{-1} b_2 \in A \Leftrightarrow (b_1 N)^{-1}(b_2 N) \in (A/N) \Leftrightarrow (b_1 N)(A/N) = (b_2 N)(A/N)$. 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 $< A, B > /N \subset < A/N, B/N >$ stačí ověřit $xN \subset < A/N, B/N >$ 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 $< A/N, B/N > \subset < A, B > /N$ stačí ověřit, že $xN \in A/N$ nebo $xN \in B/N$ implikuje $x \in < A, B >$. Nechť tedy $xN \in A/N$, pak $xN = aN$ pro nějaké $a \in A$, tudíž $a^{-1}x \in N \subset A \subset < A, B >$ a stejně pro $xN \in B/N$.
4) Stejné jako bod 3.
5) Předpokládejme nejprve $A \trianglelefteq G$. Pak pro $aN \in A/N$ platí $gNaNg^{-1}N = gag^{-1}N = a_1 N \in A/N$, tedy $A/N \trianglelefteq G/N$.
Obrácená implikace: Nechť $A/N \trianglelefteq G/N$. Definujme zobrazeni $\sigma : G \to (G/N)/(A/N) : g \mapsto (gN)(A/N)$. 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 **??** *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 $p \nmid |x|$. Buď $N =< x >$. Jelikož G je abelovská, pak $N \trianglelefteq G$ a z Lagrangeovy věty máme $|G/N| = \frac{|G|}{|N|}$, respektive $|G/N||N| = |G|$. Protože $|N| > 1$, musí platit $|G/N| < |G|$. Dále jelikož $p \mid |G|$, ale $p \nmid |N|$, musí platit $p \mid |G/N|$. Z indukčního předpokladu pak G/N obsahuje prvek $\bar{y} = yN$ řádu p. Označme řád prvku y v G roven m. Pak jistě $(yN)^m = y^m N = eN$ proto $p \mid |y|$ a dostáváme se k předchozímu případu. $\square$

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) $e = N_0 \leq N_1 \leq \ldots \leq N_{k-1} \leq N_k = G$ 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)

Buď $G \neq e$ konečná grupa. Pak:

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

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1} \quad 1 \leq i \leq r. \tag{12}$$

Důkaz J–H první část.

Mějme nejdelší možný řetěz normálních podgrup podgrup

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

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 $\pi : N_{i+1} \to N_{i+1}/N_i$, pak ze 4.VOI 9 plyne $\pi^{-1}(H) \trianglelefteq N_{i+1}$ a N_i je jádro projekce $\tilde{\pi} : \pi^{-1}(H) \to N_i$, 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 7. □

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 $r = 1, \dots n-1 \to n$: 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

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

$\square$

Důkaz.

Díky indukčnímu předpokladu platí $r-1=t+1=s-1$ (stejné délky řetězů), 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

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

□

Corollary

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