7. kapitola. Třída konjugovaných prvků. Normalisátor prvku. Třídová rovnice. Konjugované permutace. Jednoduchost alternující grupy A_n pro $n > 4$

In: Ladislav Rieger (author): O grupách. (Czech). Praha: Mladá fronta, 1974. pp. 101–[120].

7. kapitola

TŘÍDA KONJUGOVANÝCH PRVKŮ. NORMALISÁTOR PRVKU. TŘÍDOVÁ ROVNICE. KONJUGOVANÉ PERMUTACE. JEDNODUCHOST ALTERNUJÍCÍ GRUPY A_n PRO $n > 4$

Při pojmu normální grupy jsme narazili na pojem konjugovaných prvků v grupě (prvek y byl nazván konjugovaným s prvkem x pomocí prvku z, jestliže platilo

$$y = zxz^{-1})$$

Vzájemná konjugovanost prvků je jakási příbuznost, která dovoluje rozdělit důležitým způsobem prvky grupy do oddělených tříd vzájemně konjugovaných prvků (dle zcela jiného hlediska než rozdělení do levých tříd dle podgrupy).

Utvoříme-li totiž v grupě skupiny vzájemně konjugovaných prvků, pak zřejmě každý prvek grupy leží v (alespoň) jedné skupině a žádný neleží ve dvou či více skupinách současně. Neboť jakmile by prvek z byl konjugován jednak s prvkem x, jednak s prvkem y, čili jakmile by $z_1 x z_1^{-1} = z_2 y z_2^{-1}$, pak by

$$y = z_2^{-1} z_1 x z_1^{-1} z_2 = z_2^{-1} z_1 x (z_2^{-1} z_1)^{-1}$$

takže x by bylo konjugováno s y. Každá grupa G se tedy skutečně rozpadá ve třídy vzájemně konjugovaných prvků.

Některé třídy mohou ovšem obsahovat jen jediný

prvek. Především je jednotkový prvek j (v grupě G) konjugován sám se sebou, protože $xjx^{-1} = j$. V Abelových grupách je rozdělení do tříd konjugovaných prvků zřejmě nezajímavé, každá třída vzájemně konjugovaných prvků se tam skládá z jediného prvku.

Důležité je, že *počet vzájemně konjugovaných prvků je vždy dělitelem řádu grupy* (jestliže ovšem jde o grupu konečnou).

Abychom to ukázali, uvažme k danému prvku a konečné grupy G souhrn všech prvků x, které splňují vztah $a = xax^{-1}$, tj. $ax = xa$. (Říkáme, že x je prvek komutativní s prvkem a.) Mezi takové prvky patří předně jednotka j naší grupy G. Jestliže $a = x_1ax_1^{-1}$, $a = x_2ax_2^{-1}$, pak dosazením máme

$$a = x_1x_2ax_2^{-1}x_1^{-1} = x_1x_2a(x_1x_2)^{-1}$$

takže se dvěma prvky x_1 a x_2 i jejich součin x_1x_2 je komutativní s daným prvkem a. Konečně jestliže $a = xax^{-1}$, pak $x^{-1}ax = a$, čili spolu s x též inversní prvek x^{-1} je komutativní s a. Můžeme tedy říci, že *souhrn všech prvků komutativních s daným prvkem a z grupy G tvoří podgrupu N_a grupy G*, tzv. **normalizátor prvku a** v grupě G.

Všimněme si nyní levé třídy yN_a libovolného prvku y podle normalisátoru N_a prvku a. Ukazuje se, že všechny prvky yx z takové levé třídy skýtají týž k a konjugovaný prvek yay^{-1}. Neboť $yxa(yx)^{-1} = y(xax^{-1})\,y^{-1} = yay^{-1}$, podle definice normalisátoru N_a.

To tedy znamená, že různých konjugovaných prvků k prvku a je právě tolik, kolik je levých tříd v grupě G podle normalisátoru N_a, což je opravdu číslo, dělící (dle věty 3) řád grupy G.

Z toho tedy celkem vyplývá tento závěr:

Řád n konečné grupy G je součtem některých svých dělitelů, z nichž každý znamená počet vzájemně konjugovaných prvků v jedné třídě; mezi těmito děliteli, které se mohou i několikrát opakovat, vystupuje vždy číslo 1 jakožto počet všech prvků, konjugovaných s jednotkou grupy. To je slovní vyjádření tzv. třídové rovnice pro konečné grupy

$$n = 1 + h_2 + h_3 + \ldots + h_r$$

kde n je řád grupy, která se rozpadá do r tříd vzájemně konjugovaných prvků, při čemž i-tá třída obsahuje h_i prvků ($i = 1, 2, \ldots, r$) a první třída obsahuje jen jednotku grupy.

Všimněme si ještě jedné významné okolnosti, že totiž *řád každé normální podgrupy v dané grupě je součtem čísla 1 a některých ze sčítanců h_2 až h_r*, neboť normální podgrupa obsahuje ovšem jednotku grupy a s každým dalším svým prvkem obsahuje k němu i všechny prvky s ním konjugované. To je fakt, jehož se často využívá při hledání normálních podgrup dané konečné grupy.

Nyní se vraťme k permutacím, abychom viděli užití právě zavedených pojmů.

Budiž π nějaká permutace čísel $1, 2, \ldots, n$, převádějící číslo k v číslo $\pi(k)$. Pak libovolná s ní konjugovaná permutace $\varrho\pi\varrho^{-1}$ převádí číslo k v číslo $\varrho\pi\varrho^{-1}(k)$, tj. číslo $k = \varrho(i)$ v číslo $\varrho\pi\varrho^{-1}(\varrho(i)) = \varrho\pi(i)$. Čili provést permutaci $\varrho\pi\varrho^{-1}$ konjugovanou s permutací π pomocí permutace ϱ je totéž, jako současně v horní i dolní řádce rozepsané permutace π zaměnit tam stojící čísla podle permutace ϱ, tj.

$$\varrho\pi\varrho^{-1} = \begin{pmatrix} \varrho(1) & \varrho(2) & \ldots & \varrho(n) \\ \varrho\pi(1) & \varrho\pi(2) & \ldots & \varrho\pi(n) \end{pmatrix}$$

(Potřebujeme-li, přejdeme ovšem snadno k takovému vypsání, kde v první řádce jdou čísla podle velikosti.)

Např. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$, $\varrho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

$$\pi\varrho\pi^{-1} = \begin{pmatrix} 3 & 2 & 4 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Avšak permutace, konjugované k dané permutaci a jejich počet lze ještě lépe přehlédnout pomocí tzv. rozkladu permutace v oddělené cyklické permutace, stručně v oddělené cykly. Cyklem $(i_1, i_2, \ldots, i_k)$ rozumíme při tom permutaci, která převádí číslo i_1 v číslo i_2, číslo i_2 v číslo i_3, atd. až číslo i_{k-1} v číslo i_k a číslo i_k zpět v číslo i_1, kdežto ostatní (nevyznačená) čísla nechává stát. Počet k čísel, která nepřejdou v sebe sama cyklickou permutací $(i_1, i_2, \ldots, i_k)$, nazýváme délkou cyklu. Cykly délky 2 (tvaru (ik)) se nazývají transposice; znamenají změnu čísla i v číslo k a čísla k v číslo i, při čemž ostatní čísla zůstávají stát. Dva cykly nazýváme oddělenými, jestliže není žádného čísla, které by se měnilo jak při jednom tak při druhém cyklu.

Dokážeme si tuto poučku:

Každá neidentická permutace stupně n (na n-číslech $1, 2, \ldots, n$) se dá jednoznačně rozložit v součin oddělených cyklů, při čemž na pořadí činitelů nezáleží.[24])

Budiž tedy π jakákoli neidentická permutace, provedená na číslech $1, 2, \ldots, n$. Najděme si první číslo i_1, které nezůstává stát při permutaci π, $\pi(i_1) \neq i_1$. Pak se mezi čísly $\pi(i_1), \pi^2(i_1), \pi^3(i_1), \ldots, \pi^t(i_1), \ldots$ musí některá opakovat, protože všech permutovaných čísel je jen konečně mnoho. Jestliže $\pi^r(i_1) = \pi^s(i_1)$ pro $r > s$; r, s celá kladná, pak $\pi^r(\pi^s)^{-1} = \pi^{r-s}(i_1) = i_1$.

[24]) Pochopitelně pro $n = 1$ máme pouze jedinou, a tedy identickou permutaci. — Pozn. red.

Existují tedy celá kladná čísla m taková, že $\pi^m(i_1) = i_1$. Budiž k nejmenší z takových čísel. Pak čísla $i_1, \pi(i_1), \pi^2(i_1), \ldots, \pi^{k-1}(i_1)$ jsou navzájem různá, avšak $\pi^k(i_1) = i_1$ (poprvé). Čísla i_1, $i_2 = \pi(i_1)$, $i_3 = \pi^2(i_1)$, $\ldots$, $i_k = \pi^{k-1}(i_1)$ skládají cyklus délky k, který působí patrně na ně právě tak, jako celá permutace π. Jestliže již není dalšího čísla, které se permutací π mění, jsme hotovi. V opačném případě proveďme s dalším číslem, které označme třebas m_1, totéž, co před tím s číslem i_1, takže obdržíme další cyklus, řekněme $(m_1 m_2 \ldots m_q)$, kde $m_2 = \pi(m_1)$, $m_3 = \pi^2(m_1)$, $\ldots$, $n_q = \pi^{q-1}(m_1)$, kdežto $\pi^q(m_1) = m_1$ (poprvé). Opět se daná permutace π a cyklus $(m_1 m_2 \ldots m_q)$ shodují co do svého účinku na čísla $m_1, \ldots . m_q$. Jedno a totéž číslo nemůže vystupovat v obou cyklech, protože jinak bychom měli $\pi^a(i_1) = \pi^b(m_1)$ při vhodných mocnitelích a, b, takže by číslo $m_1 = \pi^{a-b}(i_1)$ náleželo do prvního cyklu, proti předpokladu. Budeme-li tento postup opakovat tolikrát, kolikrát je možno, dosáhneme (následkem konečného počtu permutovaných čísel) nakonec toho, že všechna čísla, která danou permutací π nepřecházejí v sebe sama, se rozdělí do jednotlivých cyklů. Připomeňme znova, že každý takto získaný cykl je permutace, nechávající stát všechna čísla, kromě těch, která v cyklu vystupují — a čísla v cyklu vystupující zaměňuje stejně jako rozkládaná permutace. Konečně je zřejmo, že oddělenost cyklů, tj. okolnost, že žádné dva různé cykly nehýbají týmž číslem, má za následek jejich vzájemnou komutativitu. Tím je naše tvrzení dokázáno. Následující příklady na rozklad permutace v součin oddělených cyklů si dle potřeby čtenář pro větší jistotu sám doplní dalšími. (Pozor na to, že provedením cyklu —tj. cyklické permutace—na samotných číslech cyklu dostáváme týž cykl, jen jinak psaný!)

$$\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix} = (1\,3\,4\,2)\,[= (3\,4\,2\,1) = (4\,2\,1\,3) = (2\,1\,3\,4)]$$

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\10&4&5&9&1&8&7&2&6&3\end{pmatrix} =$$

$$= (1\ 10\ 3\ 5)\,(2\ 4\ 9\ 6\ 8)\,[= (4\ 9\ 6\ 8\ 2)\,(3\ 5\ 1\ 10) = \ldots]$$

(Je třeba pamatovat na to, že k určení permutace jejím rozkladem v cykly je třeba udat počet permutovaných předmětů (čísel), které jsou v cyklickém rozkladu vyznačeny.)

Podle předchozího nyní určíme permutaci $\varrho\pi\varrho^{-1}$, konjugovanou s permutací π pomocí permutace ϱ nejjednodušeji, je-li π dána rozkladem v oddělené cykly. Pak prostě nahradíme v takovém cyklickém rozkladu každé číslo i číslem $\varrho(i)$ a obdržíme tak konjugovanou permutaci $\varrho\pi\varrho^{-1}$ v rozkladu v oddělené cykly. Tak např., je-li π posléze uvedená permutace a ϱ je permutace

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\5&6&10&7&8&9&2&3&4&1\end{pmatrix}$$

pak v cyklickém rozkladu lze psát pohodlně

$$\varrho\pi\varrho^{-1} = (5\ 1\ 10\ 8)\,(6\ 7\ 4\ 9\ 3)$$

Samozřejmě tedy má konjugovaná permutace s danou permutací stejný počet cyklů téže délky. Ale patrně též obráceně, jestliže dvě permutace vykazují ve svých rozkladech v oddělené cykly týž počet cyklů stejné délky (pro každou se vyskytující délku cyklu), pak jsou tyto permutace vzájemně konjugované — a to pomocí každé permutace, která převádí vždy čísla jednoho cyklu v jedné permutaci v čísla cyklu téže délky v druhé permutaci.

Každou cyklickou permutaci možno dále ještě rozložit v transposice (dvojčlenné cykly), ovšem nikoli již oddělené, nýbrž naopak, navazující na sebe. Jestliže

$(i_1 i_2 \ldots i_k)$ je daný cyklus, pak patrně permutace jím dosažená je rovna sledu postupně provedených výměn (transposic) tak, že možno psát

$$(i_1 i_2 \ldots i_k) = (i_1 i_2)\,(i_2 i_3) \ldots (i_{k-2} i_{k-1})\,(i_{k-1} i_k)$$

[Pozor na to, že čteme a násobíme *od prava doleva*. Nejdříve si všimněme, že i_k přechází v i_{k-1} první transposicí, pak i_{k-1} přechází v i_{k-2} druhou transposicí atd., až posléze tento řetězec změn končí změnou i_2 v i_1, takže celý součin transposic převede i_k v i_1. Avšak pokud jde o i_{k-1}, již (zprava) první transposice převádí i_{k-1} v i_k a v žádné z následujících transposic se i_k už nevyskytuje, takže celkem náš součin transposic převádí i_{k-1} v i_k. Podobně dále i_{k-2} bude měněno až po připojení druhé (zprava) transposice, a to v i_{k-1}, kteréžto číslo již zůstane stát i po provedení dalších transposic. Stejně zjistíme i u ostatních čísel, že vypsaný součin transposic na ně účinkuje tak jako první transposice (zprava), v níž se toto číslo vyskytuje, tedy tak jako sám cykl.]

Z rozkladu cyklu v transposice vyplývá, že cykl o sudé délce je permutace lichá, jakožto součin lichého počtu transposic (což jsou permutace liché), a cykl o liché délce je permutace sudá, jakožto součin sudého počtu transposic (viz par. 5).

A nyní se obraťme k alternující grupě A_5 všech sudých permutací stupně 5.

Věta 10

Alternující grupa A_5 (sudých permutací z pěti předmětů) je jednoduchá.

Důkaz provedeme metodou, o níž již byla zmínka: určíme počet permutací ve třídách vzájemně konjugovaných permutací, na něž se rozpadá grupa A_5, a ukážeme prostě, že z čísla 1 a některých sčítanců, udávají-

cích počet konjugovaných permutací v A_5, nelze obdržet součet, který by dělil řád grupy A_5, tj. číslo, jež by mohlo být řádem normální podgrupy. Při tom musíme dát pozor na to, že půjde o konjugovanost v A_5 (a nikoli v S_5), tj. o konjugovanost pomocí sudých permutací.

Podle rozkladu v oddělené cykly nalézáme tyto druhy sudých permutací stupně 5 — jichž je $\frac{1}{2}5! = \text{řád } A_5 = 60$ (vedle identické permutace):

1. Součiny dvou (oddělených) cyklů, což musí být dvojčlenné cykly (transposice), aby permutace byla sudá
2. Jednotlivé trojčlenné cykly
3. Jednotlivé pětičlenné cykly

K 1. Všechny součiny dvou oddělených transposic, tedy permutace tvaru $(a_1a_2)\,(b_1b_2)$, (kde a_1, a_2, b_1, b_2 jsou různá čísla od 1 do 5), jsou konjugované se sudou permutací (1 2) (3 4) — a jsou tedy konjugované i navzájem. Neboť jedna z obou permutací

$$\begin{pmatrix}1&2&3&4&5\\a_1&a_2&b_1&b_2&c\end{pmatrix},\quad \begin{pmatrix}1&2&3&4&5\\a_2&a_1&b_1&b_2&c\end{pmatrix}$$

(c je jediné zbývající číslo různé od čísel a_1, a_2, b_1, b_2) je zaručeně sudá a pomocí obou obdržíme permutaci $(a_1\,a_2)\,(b_1\,b_2)$ jakožto konjugovanou k permutaci (1 2) (3 4) (dle svrchu uvedeného). Tvoří tedy součiny dvou oddělených transposic právě jednu třídu navzájem konjugovaných permutací v grupě A_5. Jejich počet obdržíme, kombinujíce každou z $\binom{5}{2}$[24]) dvojic čísel s $\binom{3}{2}$ zbý-

[24]) $\binom{n}{k}$ je ze školy známý binomický koeficient

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{1.2.3\ldots k}.$$

vajícími dvojicemi a dělíce dvěma, protože takto obdržíme každý součin dvou oddělených transposic dvakrát. Tedy první třída vzájemně konjugovaných permutací v grupě A_5 obsahuje $\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$ prvků.

K 2: Se třemi danými čísly a, b, c lze provést právě dva různé cykly, $(a\ b\ c)$ a $(b\ a\ c)$. Máme tedy $2 . \binom{5}{3} = 20$ trojčlenných cyklů v A_5. Ty jsou však všechny konjugované k cyklu (1 2 3), protože jedna z permutací

$$\begin{pmatrix}1&2&3&4&5\\a&b&c&d&e\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5\\a&b&c&e&d\end{pmatrix} \text{ a } \begin{pmatrix}1&2&3&4&5\\b&a&c&d&e\end{pmatrix},\ \begin{pmatrix}1&2&3&4&5\\b&a&c&e&d\end{pmatrix}$$

kterou žádané konjugovanosti lze dosáhnout, je jistě sudá. Druhá třída navzájem konjugovaných permutací v A_5 obsahuje tedy 20 prvků.

K 3: Pět čísel lze podrobit celkem $\frac{1}{5}5! = 24$ cyklickým permutacím, protože spolu s jedním pořadím pěti čísel i pět dalších pořadí, získaných z daného tou cyklickou záměnou, která je daným pořadím vyznačena, dává zápis téhož cyklu. (Na rozdíl od předchozího, nejsou všechny pětičlenné cykly vzájemně konjugovány v grupě A_5.) Je vidět, že jedinými permutacemi, pomocí nichž pětičlenný cykl je konjugován sám se sebou, je tento cykl sám a jeho mocniny. Jinými slovy, normalizátor pětičlenného cyklu v A_5 je tvořen právě všemi pěti různými mocninami tohoto cyklu. Ještě jinak řečeno, třída všech v grupě A_5 konjugovaných permutací k pětičlennému cyklu obsahuje

$$\frac{\text{řád } A_5}{5} = \frac{60}{5} = 12 \text{ permutací}$$

Rozpadá se tedy všech 24 pětičlenných cyklů v A_5 do dvou takových tříd vzájemně konjugovaných, obě po 12 permutacích (prvcích grupy A_5).
Třídová rovnice pro alternující grupu A_5 tedy zní

$$\tfrac{1}{5}5! = 60 = 1 + 15 + 20 + 12 + 12$$

Jako řády (netriviální) normální podgrupy v A_5 by tedy přicházela v úvahu jenom tato čísla (dle svrchu řečeného):

$$12 + 1 = 13,\ 15 + 1 = 16,\ 20 + 1 = 21$$
$$12 + 12 + 1 = 25,\ 15 + 12 + 1 = 28$$

Z nich však ani jedno neobstojí, nejsouc dělitelem řádu grupy, tj. čísla 60. — Tedy skutečně alternující grupa A_5 nemůže mít netriviálních normálních podgrup.
Ukazuje se, že všechny další alternující grupy jsou jednoduché. Myšlenku důkazu tohoto na první pohled překvapujícího jevu založíme, zhruba řečeno, v tomto: Na jedné straně netriviální normální podgrupa alternující grupy musí obsahovat dosti mnoho permutací, protože s každou permutací musí obsahovat značnou rozmanitost všech konjugovaných permutací. Na druhé straně však z předpokladu jednoduchosti alternující grupy A_n (která je ovšem podgrupou následující alternující grupy A_{n+1}) vyplývá (užitím 2. věty o isomorfismu), že naopak netriviální normální podgrupa v A_{n+1} musí obsahovat „velmi málo" permutací; z tohoto rozporu vyplývá, že nemá-li A_n netriviálních normálních podgrup, nemá je ani A_{n+1}. Protože však alternující grupa A_5, jak již víme, jednoduchá je, je jednoduchá i následující alternující grupa A_6, následkem toho je jednoduchá i další alternující grupa A_7, atd., až do nekonečna.
Náš postup důkazu jednoduchosti alternujících grup.

stupně vyššího než pátého, který následuje, je tedy tzv. *induktivním* postupem.

Věta 11

Alternující grupa A_n stupně n většího než čtyři je jednoduchá.

Důkaz: Alternující grupa A_5 je jednoduchá podle předchozí věty. Kdyby některá z dalších alternujících grup A_n pro $n > 5$ nebyla jednoduchá, musela by mezi nimi být jedna alternující grupa, řekněme A_m, co nejmenšího stupně m (ovšem že je $m > 5$) taková, že ona sama již jednoduchá není, ale předchozí alternující grupa A_{m-1} ještě jednoduchá je. Ukážeme, že existence takové první nikoli jednoduché alternující grupy A_m je vyloučena, protože by vedla k odporujícím si důsledkům.

Předpokládejme tedy, že máme v alternující grupě A_m ($m > 5$) netriviální normální podgrupu N (která tedy obsahuje více než jenom identickou permutaci).

Prvním naším (pomocným) krokem bude nalézt v N vhodnou permutaci ϱ a dvě z permutovaných čísel, řekněme i a k tak, aby čísla i, k, $\varrho(i)$, $\varrho(k)$ byla různá. — Zvolme proto v N libovolnou neidentickou permutaci σ, převádějící číslo i v číslo $\sigma(i) \neq i$ a rozložme σ v součin oddělených cyklů, jak byla o tom řeč shora. Jsou tři možnosti (vzhledem k tomu, že jde o sudé permutace):

a) máme více cyklických činitelů v rozkladu

b) rozklad se redukuje na jediný cykl, obsahující více než čtyři z permutovaných čísel

c) rozklad se redukuje na jediný, trojčlenný cykl

V obou případech a) a b) položme $\sigma = \varrho$; v případě a) pak vezmeme za i třebas libovolné číslo z prvního a za k libovolné číslo z druhého cyklu rozkladu, takže i, k, $\varrho(i)$, $\varrho(k)$ jsou zřejmě různá čísla. V případě b) vezmeme

třebas za i první a za k třetí číslo uvažovaného cyklu, takže $\varrho(i)$ bude druhé a $\varrho(k)$ čtvrté číslo tohoto cyklu, tedy opět jistě různá čísla.

V případě c) nechává permutace σ stát všechna čísla kromě tří. Můžeme pro jednoduchost předpokládat, že jde o čísla 1, 2, 3 a že $\sigma = (1\ 2\ 3)$ (toho lze vždy dosáhnout vhodným přečíslováním permutovaných předmětů). Konjugováním pomocí sudé permutace $(2\ 5)\ (1\ 4)$ (kterou dle předpokladu $m > 5$ máme k dispocici) zjišťujeme v naší normální podgrupě N přítomnost permutace

$$(2\ 5)\ (1\ 4)\ (1\ 2\ 3)\ (1\ 4)^{-1}\ (2\ 5)^{-1} = (4\ 5\ 3)$$

a tedy a přítomnost permutace

$$\varrho = (4\ 5\ 3)\ (1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & m \\ 2 & 4 & 1 & 5 & 3 & 6 & \dots & m \end{pmatrix} = (1\,2\,4\,5\,3)$$

Tím je případ c) převeden na případ b), který jsme již vyřídili.

Tedy opravdu máme vždy permutaci ϱ v N takovou, že čísla i, k, $\varrho(i)$, $\varrho(k)$ jsou různá.

Nyní provedeme druhý krok. Ten spočívá v důležitém zjištění, že z permutovaných čísel kterákoli dvě různá čísla r, s lze převést vhodnou permutací ϱ^*, obsaženou v N, v kterákoli dvě čísla r', s' (z permutovaných čísel) — pokud jen jsou čísla r, s, r', s' různá.

Za tím účelem si najdeme sudou permutaci π (v A_m), která převádí číslo i v číslo r, číslo k v číslo s, číslo $\varrho(i)$ v číslo r' a číslo $\varrho(k)$ v číslo s'[25]). Takovou sudou permutaci π si snadno sestrojíme prostě tak, že ještě určíme zcela libovolně v co mají přejít zbývající čísla — to jsou

[25]) Kdybychom nevěděli, že i, k, $\varrho(i)$, $\varrho(k)$ jsou různá čísla, nemohli bychom vždy s úspěchem permutaci π určit tak, jak to (níže) potřebujeme.

podle předpokladu ($m > 5$) alespoň ještě dvě — a není-li již takto daná hledaná permutace sudá, pak výměnou dvou naposled nahrazovaných čísel dosáhneme sudosti žádané permutace π.

Nyní však konjugovaná permutace $\varrho^* = \pi\varrho\pi^{-1}$, patřící spolu s ϱ do naší normální podgrupy N, převádí vskutku číslo r v číslo $\varrho^*(r) = \pi\varrho\pi^{-1}(r) = \pi\varrho\pi^{-1}\pi(i) = \pi(\varrho(i)) = r'$, a číslo s v číslo $\varrho^*(s) = \pi\varrho\pi^{-1}(s) = \pi\varrho\pi^{-1}\pi(k) = \pi(\varrho(k)) = s'$.

Tento krok nám již dovoluje udat číslo, jež musí být překročeno nebo alespoň dosaženo řádem naší normální podgrupy. Shledáváme totiž, že v N musí být $m - 3$ permutací, jimiž číslo 1 přechází v číslo 2 a při tom číslo m přejde v jedno z $m - 3$ zbývajících čísel. Stejně však musí N obsahovat dalších $m - 3$ permutací, převádějících číslo 1 v číslo 3 a současně číslo m ve zbývající čísla. Podobně vždy dalších $m - 3$ permutací v N je zaručeno při přechodu čísla 1 v čísla 4, 5, ..., m. Celkem tedy obsahuje naše normální podgrupa N nejméně $(m - 3)(m - 1)$ různých permutací; řád grupy N musí dosáhnout anebo překročit číslo

$$(m - 3)(m - 1) = m^2 - 4m + 3$$

A nyní se obraťme k obrácenému dohadu (se shora) řádu naší normální podgrupy.

K tomu užijeme 2. věty o isomorfismu. Pokládáme za podgrupu U (z věty 9) předchozí alternující grupu A_{m-1} všech těch sudých permutací na m předmětech (číslech), které nechávají jistý předmět (číslo) stát; za normální podgrupu N ve větě 9 vezmeme ovšem N a za celou grupu G samozřejmě celou alternující grupu A_m. Pak máme isomorfismus

$$A_{m-1}/(A_{m-1} \cap N) \cong (A_{m-1}N)/N$$

kde si zatím ještě ponecháváme možnost stanovit předmět (číslo), jejž mají nechat stát permutace z A_{m-1}. Průnik $A_{m-1} \cap N$ značí normální podgrupu v grupě A_{m-1} všech permutací, jež patří jak do A_{m-1}, tak i do naší normální podgrupy N.

Předmět, tj. číslo, které mají nechat stát permutace z A_{m-1}, si nyní zvolíme tak, aby podgrupa N, (která byla předpokládána jako netriviální, tj. různá od celé grupy A_m), neobsahovala podgrupu A_{m-1}, čili aby průnik $A_{m-1} \cap N$ nebyl roven A_{m-1}. Že to vždy lze (za našich předpokladů), to poznáme takto: V opačném případě by N musela obsahovat každou z možných podgrup A_{m-1} (pro různě zvolená, při permutacích stálá čísla), tj. N by obsahovala veškeré sudé permutace (na našich m předmětech, resp. číslech), které nechávají stát aspoň jedno číslo. Jakožto podgrupa obsahovala by N veškeré součiny takových permutací. Avšak tím by již N obsahovala všechny sudé permutace (stupně m) vůbec. Neboť rozložme každou z dalších sudých permutací (tj. takových, které nenechávají stát nic) v součin oddělených cyklů. Dále rozložme tyto cykly v součiny transposic (tak jak jsme to uvedli shora) a konečně sdružme tyto (více než tři) posléze získané činitele (transposice) do dvou činitelů vždy o sudém počtu transposic. Tak se stává opravdu sudá permutace součinem dvou sudých permutací, z nichž každá nechává aspoň jedno permutované číslo stát.

Zvolivše si tedy podgrupu A_{m-1} v A_m tak, aby nebyla obsažena v normální podgrupě N, máme v průniku $A_{m-1} \cap N$ normální podgrupu (pod)grupy A_{m-1}, která je od A_{m-1} různá. Avšak A_{m-1} je podle předpokladu ještě jednoduchá grupa, tedy nezbývá než že $A_{m-1} \cap N$ se redukuje na pouhou jednotku (identickou permutaci).

Následkem toho však faktorová grupa $A_{m-1}/(A_{m-1} \cap N)$ je prostě grupa A_{m-1} sama. Nahoře naznačený isomorfismus nám tedy mimo jiné praví to, že faktorová grupa $(A_{m-1}N)/N$ má týž řád, jako má A_{m-1}, což je číslo $\frac{(m-1)!}{2}$; toto číslo je tedy rovno řádu grupy $A_{m-1}N$ dělenému řádem normální podgrupy N (viz věta 5). Avšak řád grupy $A_{m-1}N$ jakožto podgrupy v A_m je nanejvýše roven číslu $\frac{m!}{2}$ (což je řád A_m). Máme tedy

$$\frac{(m-1)!}{2} \leqq \frac{m!}{2} \frac{1}{\text{řád } N}$$

z čehož plyne, že řád naší normální podgrupy N grupy A_m je nanejvýše roven číslu m.

Avšak prve jsme dokázali, že řád grupy N musí být větší anebo nejvýše roven číslu $m^2 - 4m + 3$. Z toho ovšem vyplývá, že $m^2 - 4m + 3 \leqq m$, tj. že číslo

$$m - (m^2 - 4m + 3) = 5m - (m^2 + 3)$$

je nezáporné, čili i číslo

$$(5m - [m^2 + 3]) : m = 5 - \left(m + \frac{3}{m}\right)$$

je nezáporné. Ale to právě není pro předpokládané $m > 5$ možné. Dospěli jsme tedy k hledanému logickému rozporu, plynoucímu z předpokladu, že existuje alternující grupa A_m pro $m > 5$, která by nebyla jednoduchá; tím je tedy takový předpoklad vyvrácen a věta o jednoduchosti alternujících grup permutací stupně alespoň pátého dokázána.

Seznání jednoduchosti alternujících grup A_n všech stupňů n, vyšších, než 4 bylo důležitým krokem v počátcích samotné teorie grup, protože se ukázalo, jak složitými (vzhledem k rozmanitosti podgrup těchto alternujících grup) mohou být jednoduché grupy (jednoduché vzhledem k tomu, že nemají normální netriviální podgrupy). Jak jsme však již naznačili, má tento poznatek značný význam i mimo teorii grup, v tzv. Galoisově[26]) teorii algebraických rovnic tvaru

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$

tj. tzv. algebraických rovnic stupně n o jedné neznámé x. V této souvislosti byla také jednoduchost alternujících grup objevena. Není možno podat zde ani přibližný výklad Galoisovy teorie. Musíme se spokojit s pouhým poukazem na to, že Galoisova teorie převádí vlastnosti algebraické rovnice o jedné neznámé ve vlastnosti jisté tzv. Galoisovy grupy permutací kořenů této rovnice. Vlastnostem grupy odpovídají vlastnosti rovnice a naopak. Zejména řešitelnosti rovnice pomocí tzv. algebraických početních úkonů (sečítání, odčítání, násobení, dělení, mocnění, odmocňování) odpovídá jistá vlastnost (příslušné Galoisovy) grupy; tato vlastnost byla proto nazvána řešitelnost grupy. Z jednoduchosti alternujících grup stupňů vyššího než čtyři vyplývá, že Galoisova grupa obecné rovnice stupně vyššího než čtyři *není řešitelná*. Tedy neexistují byť sebe složitější vzorce, které by dovolovaly vypočítat (pomocí šesti algebraických úkonů) hodnoty jednotlivých kořenů rovnice pátého, šestého a vyššího stupně podobně, jako

[26]) Pěkný výklad Galoisovy teorie nalezne čtenář např. v polské učebnici vyšší algebry: Sierpiński, *Zarys algebry wyszej* (Monografie matematyczne Warszawa 1948) jako dodatek od prof. Mostowského.

je tomu u rovnic druhého (to čtenář zná), třetího a čtvrtého stupně (to čtenář možná nezná, ale takové vzorce pro rovnice druhého, třetího a čtvrtého stupně byly známy již počátkem novověku, viz Schwarzovu knížku „O rovnicích"). Objev neřešitelnosti rovnic stupně vyššího než čtyři algebraickým vzorcem, a co více, nalezení konkrétních příkladů rovnic s celočíselnými koeficienty, jichž žádný kořen se nedá vytvořit pomocí vyjmenovaných šesti algebraických početních úkonů, prováděných s koeficienty rovnice, patří k největším objevům algebry na počátku 19. století, na nichž se podílejí nejméně tři matematikové: Ital Ruffini, Francouz Galois a Nor Abel. Tímto objevem definitivně skončilo marné hledání vzorců pro řešení rovnic pátého a vyššího stupně, které trvalo dobrá tři staletí.

Po tomto, bez tréninku a napoprvé jistě namáhavém výstupu, který jsme krok za krokem provedli, věnujeme se nyní již jen klidnému rozhledu z relativního vrcholku, jehož jsme právě dosáhli, tj. pohledu na některé další a vyšší vrcholky teorie grup. Řečeno méně obrazně (a pro čtenáře, jenž nemá v oblibě turistiku) v další a závěrečné kapitole našeho výkladu základních pojmů teorie grup půjde již jen o informativní přehled některých hlavních výsledků a užití teorie grup, které podáme bez důkazů.

Cvičení

1. Proveďte vynásobení cyklů

a) $(1\ 4\ 2)\,(5\ 3\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} = \varrho$

b) $(3\ 5)\,(1\ 2\ 8\ 7)\,(6\ 5\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix} = \sigma$

c) Pro cykl $\pi = (1\ 2\ 3\ 4\ 5\ 6)$ udejte všechny vzájemně různé mocniny $\pi^2, \pi^3, \ldots$ (Přesvědčte se, že mocnina cyklu obecně není již jediný cykl: $\pi^2 = (1\ 3\ 5)\ (2\ 4\ 6)$; ale ovšem $(1\ 3\ 5)^3 = (1\ 5\ 3)$. *Jaké pravidlo mocnění cyklů lze vyslovit pro to, kdy se cykl mocněním rozpadá?

2. Najděte konjugované permutace

$$\varrho\pi^3\varrho^{-1},\ \sigma\varrho\sigma^{-1},\ \varrho\sigma\varrho^{-1},\ \pi^3\varrho\pi^{-3}$$

k permutacím π^3, ϱ, σ ze cvič. 1.

3. Proveďte rozdělení permutací do tříd konjugovaných pro grupy S_3 a S_4 podrobně. Napište třídové rovnice.

4. Řád permutace je nejmenším společným násobkem délek oddělených cyklů v rozkladu. — Dokažte!

5. Nazveme sudou permutaci π' všech přirozených čísel 1, 2, ... každou sudou permutaci π nějakých n čísel, která byla doplněna předpisem $\pi'(n+1) = n+1$, $\pi'(n+2) = n+2$, ... atd. bez omezení. (Zatímco $\pi'(k) = \pi(k)$ pro $k = 1, 2, \ldots, n$). Je tedy π' předpis, přiřazující každému přirozenému číslu přesně jedno přirozené číslo, při čemž jen konečně mnoho čísel obdrží tímto přiřazením číslo od daného čísla různé; (sudá permutace všech přirozených čísel nechává stát skoro všechna čísla, až na konečný počet výjimek; tato výjimečná čísla jsou podrobena jisté sudé permutaci v obvyklém smyslu).

Dokažte, že sudé permutace přirozených čísel tvoří (nekonečnou nekomutativní) grupu A při definici násobení

$$[\pi'.\varrho']\ (r) = \pi'(\varrho'(r)) \text{ pro } r = 1, 2, \ldots$$

Dokažte, že grupa A obsahuje podgrupy A_n pro $n = 1, 2, 3, \ldots$ vesměs isomorfní s grupami A_n všech sudých permutací prvních n čísel $1, 2, \ldots, n$; dále dokažte, že každý prvek z grupy A (sudá permutace přirozených čísel) je obsažen v některé z podgrup A_n.

6. *Dokažte, že nekonečná grupa A neobsahuje vlastní normální podgrupu čili že je příkladem nekonečné jednoduché grupy.

(Návod: Kdyby N byla normální podgrupa v A, pak průnik $A'_n \cap A$ by byla normální podgrupa v podgrupě A'_n (jak víme z 2. věty o isomorfii). Následkem jednoduchosti podgrup

A'_n pro $n = 5, 6, 7, \ldots$ (dle cvič. 6) musí buďto: $A'_n \cap N = A'_n$ čili A'_n je podgrupou v normální podgrupě N anebo: $A'_n \cap N$ obsahuje jen identickou permutaci (jednotku). Nastává-li druhá možnost pro všechna $n = 5, 6, 7$ pak snadno ukážete, že N obsahuje jen jednotku. V opačném případě $A'_m \cap N = A'_m$ pro jisté $m > 5$ zase snadno ukážete, že N obsahuje každou podgrupu A'_r pro $r > m$, a tedy že N je rovna celé grupě A.)

7. Dokažte jednoduchost všech alternujících grup A_n pro $n \neq 4$.