PŘÍRODOVĚDECKÁ FAKULTA UNIVERZITY PALACKÉHO
KATEDRA ALGEBRY A GEOMETRIE

BAKALÁŘSKÁ PRÁCE

Speciální vlastnosti permutací

2013 Martin Broušek

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením RNDr. Jaroslava Švrčka, CSc., a že jsem uvedl veškerou použitou literaturu.

V Olomouci 30. dubna 2013 ....

V tomto místě bych velmi rád vřele poděkoval ochotnému vedoucímu mé práce, RNDr. Jaroslavu Švrčkovi, CSc., za veškerý čas, rady a trpělivost, kterou pro mě našel.

Obsah

Úvod **5**

Seznam použitých označení **6**

1 Základní vlastnosti permutací **7**

1.1 Pojem permutace 7

1.2 Disjunktní permutace 8

1.3 Transpozice a jejich vlastnosti 11

1.4 Pojmy z teorie grup 14

2 Stopy permutací **18**

2.1 Pojem stopy 19

2.2 Kombinatorika s využitím stop 19

2.3 Stopy a konjugované permutace 23

2.4 Důsledky kombinatorických úvah 27

Závěr **29**

Literatura **30**

Úvod

Cílem této bakalářské práce je ukázat některé významné vlastnosti permutací, zejména pak ty, jež se týkají rozkladu permutací na cykly. Tento rozklad je možné zjednodušeně popsat pojmem *stopa* permutace, který má prokazatelnou souvislost s komutujícími permutacemi a také s některými vlastnostmi symetrických grup, a proto je jeho studium náplní celé druhé kapitoly.

Motivací pro tuto práci byl autorův příspěvek *O jedné vlastnosti permutací*, viz [1], ve kterém je odvozen vztah pro počet permutací komutujících s danou permutací v závislosti na její stopě. Další zkoumání problematiky rozkladu permutací na cykly nás rychle přivede na otázku, kolik existuje permutací s danou stopou. Stručnou odpověď, kterou lze najít např. i v knize [8], představuje vzorec, jenž se velmi podobá vzorci z autorova článku. Celá tato práce proto směřuje k objasnění této podobnosti, čehož je v samém závěru dosaženo sestrojením vhodné bijekce. Z provedených úvah přitom plyne také několik překvapivých důsledků popisujících vlastnosti symetrických grup.

Kromě odvození některých zajímavých speciálních vlastností permutací podává tato práce i poměrně ucelený úvod do problematiky konečných permutací, a to jak z kombinatorického, tak grupového hlediska.

Seznam použitých označení

$\mathbb{N}$	— množina přirozených čísel, tj. $\mathbb{N} = \{1, 2, 3, \ldots\}$
$\emptyset$	— prázdná množina
$\lvert A \rvert$	— mohutnost množiny A (počet prvků)
$a \in A$	— a je prvkem množiny A
$A \subseteq B$	— množina A je podmnožinou množiny B
$A \cap B$	— průnik množin A a B
$A \cup B$	— sjednocení množin A a B
$A \times B$	— kartézský součin množin A a B
$a \longmapsto b$	— prvku a odpovídá prvek b
Imf	— pro $f : A \longrightarrow B$ je $Imf = \{f(a) \in B; a \in A\}$
$n!$	— n faktoriál, tzn. $0! = 1$ a $n! = n \cdot (n-1)!$, kde $n \in \mathbb{N}$
$\square$	— konec důkazu

1 Základní vlastnosti permutací

V úvodní části práce zavedeme některé potřebné pojmy týkající se permutací, uvedeme několik základních tvrzení a zmíníme používané způsoby zápisu permutací.

1.1 Pojem permutace

Definice 1.1.1

Nechť M je neprázdná konečná množina, pak permutací *množiny M nazveme libovolné bijektivní zobrazení $g : M \longrightarrow M$.*

Poznámka. Obecně je možné zavést permutaci nekonečné množiny jako libovolnou bijekci na dané množině, avšak v celé této práci se budeme věnovat výhradně permutacím konečných množin.

Zavedeme tzv. maticový zápis permutace. Např. můžeme permutaci g množiny $M = \{1, 2, \ldots, 8\}$ zapsat ve tvaru

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

kde se v prvním řádku nacházejí vzory a v druhém jejich odpovídající obrazy. V našem příkladu, permutaci g, tedy platí $g(1) = 2$, $g(2) = 4$, atd. Často se také můžeme setkat se značením, kde první řádek této matice vynecháme, protože evidentně není nutný pro jednoznačný zápis permutace. Můžeme tedy permutaci g zapsat ve tvaru

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

Protože libovolná permutace je zobrazením na množině M, je přirozené zabývat se permutacemi na obrazech prvků, a proto v následující definici zavedeme skládání permutací.

Definice 1.1.2

Složením *permutací g, h na M rozumíme takovou permutaci $g \circ h$, v níž pro každé $a \in M$ platí $(g \circ h)(a) = h(g(a))$.*

Skutečnost, že složení dvou permutací na množině M je opět permutace na M, je zřejmá, protože složení dvou bijekcí je opět bijekce. Označme nyní G množinu všech permutací konečné množiny M.

Věta 1.1.1

Množina G spolu s operací skládání tvoří grupu.

Důkaz tohoto tvrzení nebudeme detailně provádět. Je známo, že skládání zobrazení je asociativní, jednotkou je v této grupě identické zobrazení id, tedy permutace, v níž pro každé $a \in M$ platí $id(a) = a$. Protože každá permutace g je bijektivní zobrazení, existuje inverzní zobrazení g^{-1}, které je rovněž permutací.

Definice 1.1.3

Grupu všech permutací množiny M spolu s binární operací skládání $G = (G, \circ)$ budeme nazývat symetrickou grupou *množiny M.*

Z vlastností grup plyne, že lze přirozeným způsobem zavést celočíselné mocniny permutací $g^1 = g$, $g^0 = id$, další mocniny zavedeme induktivně $g^{n+1} = g^n \circ g$ a záporné mocniny zavedeme pomocí inverzního prvku $g^{-n} = (g^n)^{-1}$. S využitím mocnin pak můžeme definovat následující pojem.

Definice 1.1.4

Konečnou množinu $O_a = \{g^n(a);\ n \in \mathbb{N}\}$ nazveme orbitou *prvku a v permutaci g.*

Podobně jako v [9] se můžeme často setkat s tím, že se orbitou rozumí posloupnost (nebo také uspořádaná k-tice) obrazů prvku a v permutacích id, g, g^2, g^3, atd. V této práci však vystačíme s pojmem orbity jako množiny. Pokud nebude podstatné, o orbitu kterého prvku se jedná, budeme hovořit jen o orbitě permutace g. Budeme-li mluvit o délce orbity, budeme mít na mysli počet prvků této orbity.

1.2 Disjunktní permutace

V této části se zmíníme o jednom vzájemném vztahu mezi permutacemi, který pak využijeme k novému způsobu jejich reprezentace. Nejprve ale zavedeme nezbytné pojmy.

Definice 1.2.1

Pevným bodem *permutace g nazveme každý prvek $a \in M$, pro něž platí $g(a) = a$.*

O počtu pevných bodů vypovídá také tzv. stupeň permutace.

Definice 1.2.2

Stupněm *permutace g množiny M rozumíme počet všech prvků konečné množiny $A_g = \{a \in M; g(a) \neq a\}$ a značíme jej $deg(g)$. Je-li $deg(g) \geq 2$, budeme o g hovořit jako o* netriviální *permutaci.*

Poznámka. Pevné body permutace g jsou tedy právě prvky všech orbit délky jedna a jejich počet je $|M| - deg(g)$.

V následující definici zavedeme jeden užitečný druh permutací.

Definice 1.2.3

Cyklem *rozumíme každou takovou permutaci g, která má nejvýše jednu orbitu O délky $|O| \geq 2$. Je-li délka $|O| = k$, pak permutaci g nazýváme* k-cyklus.

Podle této definice je identická permutace id 1-cyklem. Proto pro $k \geq 2$ budeme stejně jako u obecných permutací o k-cyklech hovořit jako o netriviálních cyklech.

Definice 1.2.4

Nechť F_g, resp. F_h je množina pevných bodů permutace g, resp. h množiny M. Řekneme, že permutace g a h jsou navzájem disjunktní*, jestliže $F_g \cup F_f = M$.*

Poznámka. Všimněme si, že permutace g a h jsou disjunktní právě tehdy, když množiny A_g a A_h, jak byly zavedeny v definici 1.2.2, jsou disjunktní.

Definice 1.2.5

Řekneme, že permutace g a h komutují*, jestliže platí $g \circ h = h \circ g$.*

Poznámka. Pro větší přehlednost budeme v dalším textu často používat také zkrácený zápis skládání permutací. Zápisem gh budeme rozumět složení $(g \circ h)$ permutací g a h, tzn. $gh(a) = (g \circ h)(a)$.

Obecně víme, že skládání permutací není komutativní, avšak pro dvojice disjunktních permutací lze dokázat následující tvrzení.

Věta 1.2.1

Disjunktní permutace komutují.

Důkaz. Nechť g a h jsou navzájem disjunktní permutace, tedy $F_g \cup F_f = M$. Pro $a \in M$ mohou nastat tři případy.

(i) Nechť $a \in F_g \cap F_h$, pak platí

$$gh(a) = h(g(a)) = h(a) = a = g(a) = g(h(a)) = hg(a)\,.$$

(ii) Nechť $a \in F_g$ a zároveň $a \notin F_h$, tedy platí $h(a) = b$, pro některé $b \neq a$. Protože h je permutace, a tedy je injektivní, musí platit $h(b) \neq b$, tzn. b není pevným bodem permutace h, a proto musí být pevným bodem g. Odtud plyne

$$gh(a) = h(g(a)) = h(a) = b = g(b) = g(h(a)) = hg(a)\,.$$

(iii) Nechť a je pevným bodem pouze permutace h. Pak analogicky $g(a) = b$, kde $b \in F_h$, a platí

$$gh(a) = h(g(a)) = h(b) = b = g(a) = g(h(a)) = hg(a)\,.$$

Tedy pro každé $a \in M$ platí $gh(a) = hg(a)$, a tedy permutace g a h komutují. □

Věta 1.2.2

Každou netriviální permutaci lze rozložit na složení po dvou disjunktních netriviálních cyklů, přičemž tento rozklad je dán jednoznačně až na pořadí cyklů.

Důkaz. Nechť g je permutace množiny M, přičemž $deg(g) \geq 2$, pak lze množinu M přirozeně vyjádřit jako sjednocení orbit permutace g, tzn.

$$M = \cup\{O_a; a \in M\}\,.$$

Přeznačme prvky množiny M tak, že $O_1, O_2, \ldots, O_k$ jsou všechny různé orbity permutace g. Pro každé $i \in \{1, 2, \ldots, k\}$ takové, že $|O_i| \geq 2$, definujme

$$g_i(a) = \begin{cases} g(a), & \text{pro } a \in O_i, \\ a, & \text{pro } a \notin O_i. \end{cases}$$

Přitom permutace g_i jsou zřejmě po dvou disjunktní netriviální cykly, protože množiny $O_1, O_2, \ldots, O_k$ jsou rovněž disjunktní. Existuje proto rozklad

$$g = g_{i_1} \circ g_{i_2} \circ \ldots \circ g_{i_p}\,,$$

kde $i_1, i_2, \ldots, i_p \in \{1, 2, \ldots, k\}$ jsou právě ty prvky, pro které platí $|O_i| \geq 2$. Tento rozklad je jediný až na pořadí cyklů, protože dle věty 1.2.1 disjunktní permutace komutují. □

Poznámka. Všimněme si, že množina $M \setminus (O_{i_1} \cup O_{i_2} \cup \ldots \cup O_{i_p})$ je právě množina F_g všech pevných bodů permutace g, a tedy cykly odpovídající množinám O_i, takovým že $|M_i| = 1$, by byly identické permutace, a proto je do rozkladu nezahrnujeme. Z této věty byla vyloučena identita, ale je zřejmé, že ji lze napsat jako složení cyklů, protože sama id je 1-cyklus, který však není netriviální.

Na základě tvrzení věty 1.2.2 je přirozené zavést také jiný způsob zápisu permutací a to zápis pomocí orbit. Permutaci

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

na množině M uvedenou jako příklad v předešlém oddíle je pak možné zapsat jako

$$g = (1\,2\,4)(3\,5)(6\,8)(7)\,,$$

kde závorky oddělují jednotlivé orbity a zobrazení uvnitř jednotlivých cyklů je vyjádřeno pořadím prvků v závorkách. V tomto zápise ale nezáleží na pořadí jednotlivých orbit. Pokud je navíc znám počet prvků množiny M, používá se občas i zápisu, kde jsou vynechány všechny pevné body.

1.3 Transpozice a jejich vlastnosti

V této části se budeme zabývat nejjednoduššími typy permutací a jejich speciálními vlastnostmi. Budeme přitom využívat poznatky z předchozího textu, zejména pak vlastnosti cyklů.

Definice 1.3.1

Libovolný 2-cyklus nazveme transpozicí.

Je zřejmé, že tento speciální typ permutací, je po identitě nejjednodušším druhem permutací, avšak oproti ní má již mnohem více netriviálních vlastností. Například evidentně platí $t^{-1} = t$ pro každou transpozici t. Pravděpodobně nejdůležitější z těchto vlastností ukazuje následující věta.

Věta 1.3.1

Každá permutace je složením transpozic.

Důkaz. Identitu můžeme zapsat ve tvaru $id = t^2$, kde t je libovolná transpozice. Každá permutace různá od identity je již stupně většího než 2. Pro netriviální permutace důkaz provedeme matematickou indukcí podle stupně permutace.

(i) Je-li permutace g stupně $deg(g) = 2$, pak je zřejmě transpozicí, a tedy tvrzení platí.

(ii) Předpokládejme, že tvrzení věty platí pro všechny permutace stupně menšího než k. Nechť $g \in G$ je permutace množiny M stupně $deg(g) = k$. Zřejmě existuje prvek $a \in M$, který není pevným bodem permutace g, tedy $g(a) = b$ pro některé $b \in M$, $b \neq a$. Uvažujme nyní transpozici $t \in G$ takovou, že $t(b) = a$ a $t(a) = b$. Pak zřejmě platí

$$gt(a) = t(g(a)) = t(b) = a\,,$$

a tedy a je pevným bodem permutace gt. Navíc, protože prvek b nebyl pevným bodem g, jsou všechny pevné body permutace g rovněž pevnými body gt, proto je $deg(gt) < k$. Podle indukčního předpokladu platí

$$gt = t_1 t_2 \dots t_s \, ,$$

kde t_1, $t_2, \dots, t_s$ jsou transpozice. Permutace $t^{-1} = t$ je opět transpozice, a proto můžeme psát permutaci g ve tvaru

$$g = gtt^{-1} = t_1 t_2 \dots t_s t^{-1} \, ,$$

tedy jako součin transpozic.

Spojením (i) a (ii) je dokázána platnost tvrzení pro permutaci libovolného konečného stupně. □

Poznámka. Lze však dokázat, že každou permutaci množiny $M = \{1, 2, \dots, n\}$ můžeme vyjádřit jako složení transpozic, které jsou pouze tvaru $(1\,i)$.

Skutečnost, že lze permutace vyjádřit jako složení permutací z dané množiny, popisuje obecněji následující definice.

Definice 1.3.2

Řekneme, že množina permutací K generuje množinu permutací H, jestliže každou permutaci h z množiny H lze vyjádřit jako složení některých permutací z K.

Poznámka. Větu 1.3.1 je tedy možné formulovat také následujícím způsobem: Množina všech transpozic generuje symetrickou grupu G.

Je důležité si uvědomit, že rozklad na součin transpozic nemusí být jednoznačný, avšak je vždy zachována parita počtu transpozic v tomto rozkladu. Vzhledem k této vlastnosti je přirozené zavést následující definici.

Definice 1.3.3

Paritou *permutace g rozumíme paritu počtu transpozic v rozkladu permutace g na transpozice.*

Poznámka. Je-li permutace složením sudého, resp. lichého počtu transpozic, budeme hovořit o sudé, resp. liché permutaci. Je zřejmé, že složením permutace s jednou libovolnou transpozicí změní paritu této permutace.

Věta 1.3.2

Množina A všech sudých permutací je podgrupou grupy G

Důkaz. Identitu můžeme psát ve tvaru $id = t^2$, kde t je libovolná transpozice, a tedy $id \in A$.

Nechť g a h jsou sudé permutace, tedy platí

$$g = t_1 t_2 \dots t_r \quad \text{a} \quad h = d_1 d_2 \dots d_s\,,$$

kde t_i a d_i jsou transpozice a r i s jsou sudá čísla. Pak platí

$$gh = t_1 t_2 \dots t_r d_1 d_2 \dots d_s\,,$$

a tedy gh je součinem $r + s$ transpozic, kde $r + s$ je rovněž sudé. Proto složení permutací g a h je sudá permutace, a tedy množina A je uzavřená na skládání.

Navíc, je-li $g = t_1 t_2 \dots t_r$, pak evidentně platí

$$g^{-1} = (t_1 t_2 \dots t_r)^{-1} = t_r^{-1} \dots t_1^{-1} = t_r \dots t_1\,,$$

a tedy $g^{-1} \in A$.

Tím je dokázáno, že množina A je podgrupou grupy G. □

Definice 1.3.4

Podgrupu A všech sudých permutací nazveme nazveme alternující *grupou.*

Stejně jako pro G je možné i pro její alternující grupu A najít jednu význačnou množinu generátorů, jak ukazuje následující věta.

Věta 1.3.3

Množina všech 3-cyklů generuje alternující grupu.

Důkaz. Pro přehlednost budeme v celém důkazu používat zápis permutací pomocí orbit, kde budeme vynechávat pevné body. Protože platí

$$(k\,i\,j) = (k\,i) \circ (j\,k)\,,$$

tak můžeme každý 3-cyklus vyjádřit jako složení dvou transpozic, a tedy všechny 3-cykly jsou sudé permutace. Proto i složení 3-cyklů je vždy sudá permutace.

Buď $g \in G$ libovolná sudá permutace, tzn. libovolná permutace z alternující podgrupy A, pak je možné ji psát jako složení sudého počtu transpozic

$$g = t_1 \circ t_2 \circ \dots \circ t_k\,,$$

které tak můžeme rozdělit do dvojic. Nyní ukážeme, že libovolnou permutaci vzniklou složením dvojice transpozic lze vyjádřit také jako složení 3-cyklů. Pro dvojici transpozic t, d rozlišíme tři případy.

(i) Nechť $t = d = (i\,j)$, pak jejich složení lze vyjádřit jako

$$t \circ d = t^2 = id = z^3 \,,$$

kde z je libovolný 3-cyklus.

(ii) Nechť $t = (i\,j)$ a $d = (j\,k)$, pak platí

$$t \circ d = (i\,j) \circ (j\,k) = (i\,k\,j) \,,$$

a tedy přímo $t \circ d$ je 3-cyklus.

(iii) Nechť $t = (i\,j)$ a $d = (k\,l)$, pak můžeme psát

$$t \circ d = (i\,j) \circ (k\,l) = (i\,j\,k) \circ (k\,i\,l) = y \circ z \,,$$

kde z a y jsou 3-cykly.

Pokud tedy v původním rozkladu permutace g nahradíme každou dvojici transpozic jí odpovídajícím složením 3-cyklů, obdržíme rozklad

$$g = z_1 \circ z_2 \circ \ldots \circ z_s \,,$$

kde z_i jsou 3-cykly. Tím je tvrzení dokázáno. □

Poznámka. Navíc lze dokázat, že alternující podgrupa A grupy G všech permutací množiny $M = \{1, 2, \ldots, n\}$, je generována všemi 3-cykly tvaru $(1\,2\,i)$.

1.4 Pojmy z teorie grup

Permutace velmi úzce souvisí s konečnými grupami, a proto v této části zaveďme alespoň nejdůležitější pojmy a základní tvrzení teorie grup. Další pojmy a tvrzení, jenž by mohly být užitečné pro lepší orientaci v základech teorie grup, můžeme nalézt např. v publikacích [7] nebo [4].

Poznámka. Pro celý tento oddíl označme G libovolnou konečnou grupu, pro kterou budeme užívat běžnou multiplikativní notaci. Dále označme e její jednotku a o počtu jejích prvků budeme hovořit jako o *řádu* grupy G. Skutečnost, že H je podgrupou grupy G, budeme zapisovat $H \leq G$.

Definice 1.4.1

Nechť $H, K \subseteq G$, pak zaveďme součin HK těchto množin jako

$$HK = \{hk \in G; h \in H,\ k \in K\} \,.$$

Je-li $H = \{h\}$, pak budeme pro přehlednost místo $\{h\}K$ psát jen hK a stejně tak místo $K\{h\}$ jen Kh.

Definice 1.4.2

Jestliže $H \leq G$ a $g \in G$, pak levou třídou*, resp.* pravou třídou*, prvku g podle podgrupy H rozumíme množinu gH, resp. Hg.*

Označme $G/_l H$ množinu všech navzájem různých levých tříd grupy G podle podgrupy H.

Věta 1.4.1

Množina $G/_l H$ tvoří rozklad grupy G na třídy.

Důkaz. Protože $e \in H$, pak pro každé $a \in G$ platí

$$a = a \cdot e \in aH\,,$$

a tedy každý prvek grupy G náleží některé levé třídě, neboli množina všech levých tříd tvoří pokrytí G.

Nechť $aH \cap bH \neq \emptyset$, pak existuje $c \in aH \cap bH$, z čehož plyne, že lze najít prvky $h_1, h_2 \in H$ takové, že $c = ah_1$ a $c = bh_2$, a tedy platí $a = bh_2h_1^{-1}$. Buď x libovolný prvek z aH, neboli $x = ah$ pro některé $h \in H$, pak platí

$$x = ah = (bh_2h_1^{-1})h = b(h_2h_1^{-1}h)\,,$$

kde však $h_2h_1^{-1}h \in H$, a proto $x \in bH$. Tím jsme dokázali, že platí $aH \subseteq bH$. Analogicky lze dokázat, že $bH \subseteq aH$, a platí tedy $aH = bH$. Odtud zřejmě plyne, že různé levé třídy jsou navzájem disjunktní. □

Stejně i pro množinu $G/_p H$ všech různých pravých tříd platí, že $G/_p H$ tvoří rozklad grupy G na třídy.

Lemma 1.4.1

Buď $H \leq G$ a $a, b \in G$, pak platí

(i) $aH = bH$, právě když $b^{-1}a \in H$,

(ii) $Ha = Hb$, právě když $ab^{-1} \in H$.

Důkaz. Důkaz provedeme jen pro tvrzení (i), neboť pro případ (ii) je důkaz analogický. Nechť platí $aH = bH$, pak $a \cdot e = a \in bH$, a tedy existuje prvek $h \in H$, pro který platí $a = bh$, a proto $b^{-1}a = h \in H$.

Naopak, nechť $b^{-1}a = h \in H$, pak platí $a = bh$, tudíž $a \in aH \cap bH$, a tedy podle věty 1.4.1 platí $aH = bH$. □

Množiny levých a pravých tříd obecně nemusí být totožné, platí ale následující věta.

Věta 1.4.2

Pro libovolnou podgrupu H grupy G platí $|G/_l H| = |G/_p H|$.

Důkaz. Definujme zobrazení $f : G/_l H \longrightarrow G/_p H$ předpisem $f(aH) = Ha^{-1}$.

Nechť $Ha \in G/_p H$ je libovolné, pak pro $a^{-1} \in G$ platí, že $f(a^{-1}H) = Ha$, a tedy f je surjektivní.

Nechť nyní $f(aH) = Ha^{-1} = Hb^{-1} = f(bH)$. Z lemmatu 1.4.1 plyne $a^{-1}b \in H$, pak ale platí

$$b^{-1}a = (a^{-1}b)^{-1} \in H\,,$$

a tedy $aH = bH$. Zobrazení f je proto injektivní, a je tedy bijekcí $G/_l H$ na $G/_p H$. $\square$

Nyní můžeme oprávněně vyslovit následující definici.

Definice 1.4.3

Počet všech levých, resp. pravých tříd rozkladu podle podgrupy H nazveme index *podgrupy H.*

Pokračujme ve výčtu společných vlastností levých a pravých rozkladů. Jak ukazuje další věta, libovolné dvě třídy mají vždy stejný počet prvků.

Věta 1.4.3

Buď $H \leq G$ a $a, b \in G$, pak platí $|aH| = |Hb|$.

Důkaz. Definujme zobrazení $f : H \longrightarrow aH$ předpisem $f(h) = ah$. Ze zavedení třídy aH je zřejmé, že f je surjekce. Nechť $f(h_1) = f(h_2)$, pak $ah_1 = ah_2$, odtud plyne $h_1 = h_2$, proto f je injekce. Tím jsme dokázali, že f je bijekce H na aH. Analogicky lze zkonstruovat bijekci $g : H \longrightarrow Hb$ a je zřejmé, že $f^{-1} \circ g$ je bijekcí aH na Hb. $\square$

Z opakovaného užití této věty plyne, že všechny levé i pravé třídy mají stejný počet prvků.

Věta 1.4.4 (J. L. Lagrange)

Nechť G je grupa řádu n a H její podgrupa řádu k a indexu i, pak platí $n = k \cdot i$.

Důkaz. Jak víme z věty 1.4.3, má každá z i tříd rozkladu grupy G podle podgrupy H právě k prvků. Protože každý z n prvků grupy G náleží do některé z těchto tříd, tak platí $n = k \cdot i$. $\square$

Důležitým důsledkem této věty je, že při hledaní podgrup grupy G se můžeme omezit jen na hledání podgrup, jejichž řád je dělitelem řádu grupy G.

Jak již bylo zmíněno výše, obecně může platit, že levé a pravé rozklady grupy G podle podgrupy H jsou různé. Stejné jsou například vždy u abelovských grup, neboť v nich pro každé $a \in G$ platí $aH = Ha$. Pro obecné grupy je však užitečné zavést následující pojem.

Definice 1.4.4

Nechť $H \leq G$. Řekneme, že H je normální *podgrupou grupy G, značíme $H \trianglelefteq G$, jestliže platí $G/_l H = G/_p H$.*

Poznámka. V abelovských grupách je tedy každá podgrupa normální.

Tato definice může být ale při důkazech poněkud neobratná, a proto je vhodné ukázat následující vlastnost normálních podgrup.

Věta 1.4.5

Podgrupa H grupy G je normální, právě když pro každé $a \in G$ a pro každé $h \in H$ platí, že $aha^{-1} \in H$.

Důkaz. Mějme normální podgrupu H grupy G a libovolný prvek $a \in G$. Protože $ae = ea = a$ a $e \in H$, pak zřejmě $a \in aH \cap Ha$, a tedy $aH = Ha$. Proto lze pro libovolný prvek $h \in H$ najít prvek $h' \in H$ tak, že platí $ah = h'a$, a tedy $aha^{-1} = h' \in H$.

Nechť naopak pro každé $a \in G$ a každé $h \in H$ platí $aha^{-1} \in H$. Zřejmě $ah \in aH$, nyní položme $h_1 = aha^{-1} \in H$, tzn. $ah = h_1 a \in Ha$, a tedy $aH \subseteq Ha$. Navíc však analogicky $ha \in Ha$, a tedy pro $h_2 = a^{-1}h(a^{-1})^{-1} \in H$ platí $ha = ah_2 \in aH$, tzn. $Ha \subseteq aH$. Z obou inkluzí plyne, že $aH = Ha$ pro každé $a \in G$ a rozklady $G/_l H$ a $G/_p H$ jsou proto totožné. $\square$

Stejně jako u jiných algebraických struktur je užitečné i pro grupy zavést speciální druh zobrazení, který zachovává všechny specifické vlastnosti grup, zejména je pak kompatibilní s grupovou operací.

Definice 1.4.5

Mějme dvě grupy $G = (G, \cdot)$ a $H = (H, \circ)$, pak zobrazení $\varphi : G \longrightarrow H$, pro něž platí

$$\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)\,,$$

nazveme homomorfizmem *z grupy G do grupy H. Je-li navíc zobrazení φ bijekce, pak jej nazýváme* izomorfizmem.

Poznámka. Ke každému izomorfizmu existuje inverzní zobrazení, které je rovněž izomorfizmem. Proto můžeme říct, že grupy G a H jsou vzájemně *izomorfní*, jestliže existuje izomorfizmus grupy G na H.

Hned v úvodu celého textu jsme zavedli pojem symetrické grupy. Nyní si však ukážeme, jak velmi úzké je spojení mezi permutacemi na konečných množinách a konečnými grupami.

Definice 1.4.6

Libovolnou podgrupu symetrické grupy nazveme permutační *grupou.*

Přestože následující věta byla původně formulována pro libovolné grupy, bude pro naši představu dostačující ji zde uvést jen pro případ konečných grup.

Věta 1.4.6 (A. Cayley)

Každá konečná grupa je izomorfní některé permutační grupě.

Důkaz. Podle definice tedy chceme ukázat, že každá konečná grupa H je izomorfní podgrupě symetrické grupy G všech permutací množiny M. Za množinu M proto vezmeme právě nosič grupy H.

Pro každé $a \in H$ definujme zobrazení $g_a : H \longrightarrow H$ předpisem $g_a(x) = xa$. Ukážeme, že všechna taková zobrazení jsou bijekce. Nechť $g_a(x) = g_a(y)$, pak platí $xa = ya$, tzn. $x = y$, a tedy g_a je injekce. Nechť $x \in H$, pak existuje prvek $xa^{-1} \in H$, pro něž zřejmě platí $g_a(xa^{-1}) = xa^{-1}a = x$, a tedy g_a je surjekce. Pro každé $a \in H$ je proto g_a bijekcí na H, neboli je permutací množiny H, tzn. $g_a \in G$.

Uvažujme nyní zobrazení $\phi : H \longrightarrow G$ dané předpisem $\phi : a \longmapsto g_a$. Buďte $a, b \in H$ takové, že $\phi(a) = \phi(b)$ pak z definice zobrazení ϕ plyne $g_a = g_b$, a proto platí

$$a = e \cdot a = g_a(e) = g_b(e) = e \cdot b = b\,,$$

tzn. že zobrazení ϕ je injektivní. Navíc však pro každé a, b, $x \in H$ platí

$$(\phi(a) \circ \phi(b))(x) = g_a g_b(x) = g_b(g_a(x)) = g_b(xa) = xab = g_a b(x) = \phi(ab)(x)\,,$$

a proto ϕ je homomorfizmus.

Protože ϕ je homomorfizmus je $K = Im\,\phi$ podgrupou v G, a tedy ϕ je hledaným izomorfizmem grupy H na permutační grupu K. □

2 Stopy permutací

V této kapitole se budeme zabývat jednou speciální vlastností permutací, která pravděpodobně nejlépe vystihuje tvar a strukturu permutací.

2.1 Pojem stopy

Dokázali jsme v části 1.2, že každou permutaci lze rozložit na složení disjunktních cyklů a že rozklad, jenž touto cestou vzniká, je jednoznačný. Je zřejmé, že různé permutace mohou mít ve smyslu rozkladu na cykly stejnou strukturu. V celém následujícím textu se budeme touto podobností zabývat a budeme zkoumat její důsledky.

Poznámka. V následujícím textu budeme G značit symetrickou grupu permutací konečné neprázdné množiny M ($|M| = n$), i když některé z uvedených vět platí i pro obecné grupy.

Definice 2.1.1

Nechť permutace $g \in G$ má právě k_1 pevných bodů, k_2 orbit délky 2, k_3 orbit délky 3 atd., až k_n orbit délky n, pak uspořádanou n-tici $(k_1, k_2, \ldots, k_n)$ nazveme stopou *permutace g.*

Z vlastností orbit plyne zřejmá vlastnost stop.

Lemma 2.1.1

Je-li $(k_1, k_2, \ldots, k_n)$ stopa permutace g množiny M, kde $|M| = n$, pak platí

$$n = k_1 + 2k_2 + 3k_3 + \ldots + nk_n \,.$$

Důkaz. Protože orbity permutace g jsou po dvou disjunktní množiny, je součet počtů jejich prvků roven počtu prvků jejich sjednocení, tedy celé množiny M. □

Odtud plyne, že každou n-tici $(k_1, k_2, \ldots, k_n)$, pro kterou platí

$$n = k_1 + 2k_2 + 3k_3 + \ldots + nk_n \,,$$

můžeme považovat za stopu nějaké permutace n-prvkové množiny.

2.2 Kombinatorika s využitím stop

Pro prvek $x \in G$ označme S_x množinu všech permutací komutujících s x a P_x množinu všech permutací, které mají s permutací x stejnou stopu.

Věta 2.2.1

Množina S_x všech permutací komutujících s permutací x je podgrupou grupy G.

Důkaz. Je zřejmé, že $id\,x = x\,id$, a tak $id \in S_x$.
Nechť g, $h \in S_x$, tedy platí $gx = xg$ a $hx = xh$ a odtud plyne

$$ghx = gxh = xgh\,,$$

a proto $gh \in S_x$. Navíc platí

$$g^{-1}x = g^{-1}xgg^{-1} = g^{-1}gxg^{-1} = xg^{-1}\,,$$

a tedy $g^{-1} \in S_x$. Proto S_x je podgrupou grupy G. □

Využitím několika kombinatorických úvah lze odvodit zajímavý vztah[1] vyjadřující závislost velikosti podgrupy S_x na stopě $k = (k_1, k_2, \ldots, k_n)$ permutace x.

Věta 2.2.2

Pro počet prvků podgrupy S_x platí

$$|S_x| = \prod_{i=1}^{n} k_i! \cdot i^{k_i}\,.$$

Důkaz. Mějme permutaci g, uvažujme některé dvě orbity O_a a O_b, kde $|O_a| = n$, $|O_b| = m$ a bez újmy na obecnosti předpokládejme, že platí $m \leq n$. Označme dále a_i ($i = 1, 2, \ldots, n$) prvky orbity O_a a b_j ($j = 1, 2, \ldots, m$) prvky O_b tak, že

$$g(a_1) = a_2,\ g(a_2) = a_3,\ \ldots,\ g(a_n) = a_1$$

a

$$g(b_1) = b_2,\ g(b_2) = b_3,\ \ldots,\ g(b_m) = b_1.$$

Hledáme-li h tak, aby platilo $g \cdot h = h \cdot g$, pak pro naše potřeby rozlišíme dva případy:

$$\text{(i)} \quad h(a_i) \notin O_a \quad \text{a} \quad \text{(ii)} \quad h(a_i) \in O_a\,.$$

(i) Nechť např. $h(a_1) = b_1$, tedy

$$hg(a_1) = g(h(x_1)) = g(b_1) = b_2$$

a mají-li permutace g a h komutovat, pak

$$b_2 = gh(a_1) = h(g(a_1)) = h(a_2).$$

Stejně pak

$$h(a_3) = b_3,\ h(a_4) = b_4,\ \ldots,\ h(a_m) = b_m,$$

[1]Uvedený výsledek byl publikován autorem v časopise Matematika–fyzika–informatika, viz [1].

dále však $\psi(a_{m+1}) = b_1$ toto je ale možné, právě když $m = n$ $(a_{m+1} \sim a_1)$.

Má-li tedy permutace h zobrazit prvek některé orbity na prvek jiné orbity, musí mít tyto orbity stejný počet prvků a také všechny zbývající prvky první orbity se musí zobrazit do téže orbity a toto zobrazení je jednoznačně určeno zobrazením zvoleného prvku.

(ii) Podobně lze postupovat i v tomto případě. Nechť např. $h(a_1) = a_3$. Platí tedy

$$hg(a_1) = g(h(a_1)) = g(a_3) = a_4.$$

Pokud ale platí $gh = hg$, pak

$$a_4 = gh(a_1) = h(g(a_1)) = h(a_2),$$

tedy $h(a_2) = a_4$, stejně tak

$$h(a_3) = a_5,\ h(a_4) = a_6,\ \ldots,\ h(a_{n-1}) = a_1,\ h(a_n) = a_2.$$

Zobrazí-li permutace h některý prvek orbity O_a na prvek téže orbity, musí analogicky zobrazit i všechny zbývající prvky orbity O_a a toto zobrazení je dáno jednoznačně zobrazením zvoleného prvku.

Je-li tedy dána permutace g a chceme určit počet $|S_x|$ všech různých permutací h takových, že $gh = hg$, rozložme nejprve orbity permutace g do skupin podle počtu jejich prvků. Z předchozích poznatků víme, že žádná taková permutace h nemůže prvek jedné skupiny zobrazit na prvek skupiny jiné a musí jej tedy zobrazit na některý z prvků výchozí skupiny. A navíc se vždy celá orbita zobrazí na celou orbitu a jednoznačnost tohoto zobrazení je zajištěna zobrazením jediného prvku.

Uvažujme tedy skupinu obsahující všechny orbity s právě p prvky, takových orbit je k_p. Existuje tak $k_p!$ možností, jak se mohou tyto orbity na sebe vzájemně zobrazit, a přitom každá z k_p orbit se může na jinou zobrazit právě p způsoby. Proto pro tuto skupinu existuje $k_p!p^{k_p}$ možností, a to nezávisle na všech ostatních skupinách. Užitím principu součinu pro všechna možná p tak dostáváme celkový počet všech možných permutací h. Platí tedy

$$|S_x| = (k_1!1^{k_1})(k_2!2^{k_2})\ldots(k_n!n^{k_n}) = \prod_{i=1}^{n} k_i!i^{k_i}$$

Tím je důkaz ukončen. $\square$

Poznámka. Libovolnou permutaci g množiny M můžeme považovat za unární operaci na M. Dvojice (M, g) je pak speciální monounární algebrou. Izomorfizmus na monounární algebře (M, x) je každé bijektivní zobrazení h na M, které zachovává operaci x, tzn. pro každé $a \in M$ platí $h(x(a)) = x(h(a))$. Evidentně je proto S_x množina všech izomorfizmů na algebře (M, x). K přístupu, kdy permutace považujeme za unární operace na M, se ještě v textu později vrátíme a využijeme jej v důkazu jednoho ze stěžejních tvrzení této práce.

Poněkud odlišnou myšlenku potřebujeme k tomu, abychom určili velikost množiny P_x.

Věta 2.2.3

Pro počet prvků množiny P_x platí

$$|P_x| = \frac{n!}{\prod_{i=1}^{n} k_i! \cdot i^{k_i}} \, .$$

Důkaz. Uvažujme permutaci x reprezentovanou zápisem pomocí jednotlivých orbit, který jsme zavedli v části 1.2. Pokud ponecháme závorky na místě a na prvcích provedeme všechny možné permutace, obdržíme zápisy $n!$ permutací se stejnou stopou jako permutace x. Tyto permutace však nemusí lišit, ale to jen ze dvou důvodů.

(i) Jednotlivé závorky reprezentující orbity délky p se celé zobrazily jedna na druhou, což se může stát právě $k_p!$ způsoby. Pokud provedeme tuto úvahu pro všechny možné délky orbit permutace x, zjistíme, že počet shod z prvního důvodu je

$$k_1! k_2! \dots k_n! \, .$$

(ii) Prvky uvnitř jednotlivých závorek orbit délky p jsou pouze cyklicky posunuté, což může nastat právě p způsoby pro jednu orbitu, tedy p^{k_p} způsoby pro všechny orbity délky p. Pro všechny délky orbit proto existuje právě

$$1^{k_1} 2^{k_2} \dots n^{k_n}$$

shod z druhého důvodu.

Proto počet permutací, jejichž stopa je shodná se stopou permutace x, je právě

$$|P_x| = \frac{n!}{k_1! 1^{k_1} \cdot k_2! 2^{k_2} \cdot \dots \cdot k_n! n^{k_n}} = \frac{n!}{\prod_{i=1}^{n} k_i! \cdot i^{k_i}} \, .$$

□

Vztahy, jenž jsme odvodili, jsou na první pohled v jistém směru podezřele podobné, a proto se nyní zabývejme objasněním této závislosti.

2.3 Stopy a konjugované permutace

Ze vztahů odvozených v předchozím oddíle a jejich důkazů je patrná jistá spojitost množin S_x a P_x, kterou se nyní budeme blíže zabývat.

Lemma 2.3.1

Pro každé dva prvky g, $h \in G$ platí

$$(h^{-1}gh)^n = h^{-1}g^n h\,.$$

Důkaz. Nechť g, $h \in G$, pak zřejmě platí

$$(h^{-1}gh)^n = \underbrace{(h^{-1}gh)(h^{-1}gh)\dots(h^{-1}gh)}_{n\text{-krát}} = h^{-1}gg\dots gh = h^{-1}g^n h\,.$$

□

Připomeňme, že se zabýváme pouze permutacemi na konečných množinách, proto v permutaci g pro každý prvek $a \in M$ existuje nejmenší přirozené číslo k takové, že $g^k(a) = a$. Číslo k zřejmě odpovídá délce orbity prvku a v permutaci g. Navíc pro každé $p \in N$ takové, že $g^p(a) = a$, platí $k|p$, což plyne jak z teorie grup, tak ze samotného zavedení permutací.

Věta 2.3.1

Mějme $g \in G$, pak permutace g a $h^{-1}gh$ mají stejnou stopu pro každé $h \in G$.

Důkaz. Nechť prvek a leží na orbitě délky n v permutaci g, tedy $g^n(a) = a$. Pak s využitím lemmatu 2.3.1 platí

$$(h^{-1}gh)^n(h(a)) = hh^{-1}g^n h(a) = g^n h(a) = h(g^n(a)) = h(a)\,,$$

tedy je-li m délka orbity prvku $h(a)$ v permutaci $h^{-1}gh$, pak nutně platí $m|n$.

Nechť naopak prvek $h(a)$ leží na orbitě délky m v permutaci $h^{-1}gh$, tedy platí $(h^{-1}gh)^m(h(a)) = h(a)$. Odtud a z lemmatu 2.3.1 plyne

$$g^m(a) = hh^{-1}g^m hh^{-1}(a) = h^{-1}((h^{-1}gh)^m(h(a))) = h^{-1}(h(a)) = a\,,$$

a tedy nutně musí platit, že $n|m$, kde n je délka orbity prvku a v permutaci g.

Proto pro každý prvek a, který v permutaci g leží na orbitě délky n, a pro každou permutaci h existuje právě jeden prvek $h(a)$, který je v permutaci $h^{-1}gh$ prvkem orbity délky n. Odtud už zřejmě plyne, že stopy permutací g a $h^{-1}gh$ jsou stejné pro každé $h \in G$. □

Právě dokázaná věta značně usnadňuje práci s prvky množiny P_x, neboť je spojuje s prvky konjugovanými s x. Díky tomuto spojení můžeme zavést užitečnou ekvivalenci na grupě G, kterou později úzce propojíme s podgrupou S_x.

Definice 2.3.1

Pro pevné x uvažujme zobrazení $\gamma_x : G \longrightarrow P_x$ dané předpisem $\gamma_x : h \longmapsto h^{-1}xh$. Označme θ_x ekvivalenci indukovanou tímto zobrazením a pro $(g, h) \in \theta_x$ budeme používat také značení $g \sim_x h$.

Poznámka. Zobrazení γ_x je zadáno korektně, protože z věty 2.3.1 plyne, že x a $h^{-1}xh$ mají stejnou stopu, a tedy $\gamma_x(h) \in P_x$ pro každé $h \in G$.

Věta 2.3.2

Pro ekvivalenci θ_x indukovanou zobrazením γ_x platí $[id]_{\theta_x} = S_x$.

Důkaz. Nechť $h \in S_x$, pak platí

$$h^{-1}xh = h^{-1}hx = x = id^{-1}x\,id\,,$$

proto $h \in [id]_{\theta_x}$, a tedy $S_x \subseteq [id]_{\theta_x}$. Naopak nechť $h \in [id]_{\theta_x}$, pak zřejmě

$$xh = hh^{-1}xh = h\,id^{-1}x\,id = hx\,,$$

a tedy $[id]_{\theta_x} \subseteq S_x$. Z obou inkluzí plyne $[id]_{\theta_x} = S_x$. □

Odtud je již zřejmé výše zmíněné spojení podgrupy S_x a ekvivalence θ_x, neboť jsme dokázali, že S_x je třídou rozkladu grupy G podle θ_x.

Lemma 2.3.2

Pro ekvivalenci platí θ_x platí, že $h \sim_x g$ právě tehdy, když $hg^{-1} \in S_x$.

Důkaz. Nechť $h \sim_x g$, tedy dle definice ekvivalence θ_x platí

$$h^{-1}xh = g^{-1}xg\,.$$

Po vynásobení této rovnosti zleva h a zprava g^{-1} obdržíme

$$xhg^{-1} = hg^{-1}x\,,$$

tedy prvek hg^{-1} komutuje s x, neboli $hg^{-1} \in S_x$. Protože provedené úpravy jsou ekvivalentní, je platnost obrácené implikace zřejmá. Proto platí, že $h \sim_x g$ právě tehdy, když $hg^{-1} \in S_x$. □

Ukažme nyní, že všechny třídy rozkladu indukovaného ekvivalencí θ_x mají stejný počet prvků.

Věta 2.3.3

Pro $g \in G$ je zobrazení $\alpha_g : S_x \longrightarrow [g]_{\theta_x}$ dané předpisem $\alpha_g : h \longmapsto hg$ bijekcí podgrupy S_x na třídu $[g]_{\theta_x}$.

Důkaz. Rozdělíme důkaz do tří částí:

(i) Nejprve ukažme, že je zobrazení α_g korektně definováno. Nechť $h \in S_x$, pak platí

$$(hg)^{-1}x(hg) = g^{-1}h^{-1}xhg = g^{-1}h^{-1}hxg = g^{-1}xg\,,$$

a tedy $hg \sim_x g$, tj. $hg \in [g]_{\theta_x}$.

(ii) Nechť $g_1 \sim_x g$, pak z lemmatu 2.3.2 plyne $g_1g^{-1} \in S_x$. A navíc platí

$$\alpha_g(g_1g^{-1}) = g_1g^{-1}g = g_1\,,$$

a tudíž pro každé $g_1 \in [g]_{\theta_x}$ existuje v zobrazení α_g vzor $g_1g^{-1} \in S_x$, tedy α_g je surjektivní.

(iii) Nechť pro $h_1, h_2 \in S_x$ platí $\alpha_g(h_1) = \alpha_g(h_2)$. Z definice zobrazení α_g plyne $h_1x = h_2x$, a proto $h_1 = h_2$, tudíž zobrazení α_g je injektivní.

□

Poznámka. Dokázali jsme tak nejen, že třídy rozkladu grupy G podle θ_x jsou stejně velké, ale zároveň také, že jsou právě pravými třídami rozkladu grupy G podle podgrupy S_x.

Abychom mohli jednoznačně propojit množinu P_x s třídami rozkladu podle θ_x, potřebujeme nyní ještě poněkud zobecnit větu 2.3.1. Ukážeme že platí i obrácená implikace.

Věta 2.3.4

Permutace g, $h \in G$ jsou konjugované, právě když mají stejnou stopu.

Důkaz. Dokážeme obě implikace.

(i) Nechť $g, h \in G$ jsou konjugované, pak z věty 2.3.1 bezprostředně plyne, že mají stejnou stopu.

(ii) Nechť mají permutace $g, h \in G$ množiny M stejnou stopu. Z každé orbity permutací g i h můžeme vybrat jeden prvek, jako zástupce této orbity. Protože g a h mají stejnou stopu, můžeme zavést zobrazení f, které každému zástupci orbity z g jednoznačně přiřadí jednoho zástupce orbity z h. Zobrazení f můžeme pak rozšířit na každý prvek $a \in M$ tak, že

$$f(g(a)) = h(f(a))\,.$$

Protože f spojuje orbity stejné délky a g i h jsou permutace, je f bijekcí a je zřejmé, že pak f je izomorfizmem monounárních algeber $\mathcal{G} = (M, g)$ a $\mathcal{H} = (M, h)$, protože způsob jeho rozšíření na celé M zajišťuje splnění podmínky homomorfizmu. Izomorfizmus f je ale zároveň bijekcí $f : M \longrightarrow M$, tudíž je rovněž permutací na množině M. Navíc z podmínky homomorfizmu plyne

$$f(g(a)) = h(f(a))$$

pro každé $a \in M$. Odtud plyne $gf = fh$, a tedy platí

$$g = fhf^{-1}\,,$$

kde $f \in G$, neboli permutace g a h jsou konjugované.

□

Poznámka. Jiný důkaz, který je založen na rozkladu permutace na sjednocení disjunktních cyklů ve smyslu tvrzení věty 1.2.2, můžeme najít v publikaci [2].

Na začátku této části jsme si všimli jistého vztahu mezi podgrupou S_x a množinou P_x. Platilo totiž, že

$$|S_x| \cdot |P_x| = |G|\,.$$

Tento vztah není nijak zřejmý, a proto tuto rovnost objasníme sestrojením odpovídající bijekce.

Věta 2.3.5

Nechť $\beta_x : P_x \times S_x \longrightarrow G$ je zobrazení dané předpisem $\beta_x : (g, h) \longmapsto fh$, kde f je pro každé $g \in P_x$ libovolný, ale pevný prvek množiny $T_g = \{k \in G;\ k^{-1}xk = g\}$. Pak zobrazení β_x je bijekce.

Důkaz. Protože permutace g a x mají stejnou stopu, jsou podle věty 2.3.4 konjugované, a tedy je množina T_g vždy neprázdná. Zobrazení β_x je tak definováno korektně.

Nechť $\beta_x((g_1, h_1)) = f_1h_1 = k$ a $\beta_x((g_2, h_2)) = f_2h_2 = k$. S využitím zobrazení $\alpha_{f_i} : S_x \longrightarrow [f_i]_{\theta_x}$ zavedeným ve větě 2.3.3 můžeme psát

$$\beta_x((g_1, h_1)) = \alpha_{f_1}(h_1) = k = \alpha_{f_2}(h_2) = \beta_x((g_2, h_2))\,.$$

Odtud je zřejmé, že $[f_1]_{\theta_x} = [f_2]_{\theta_x}$, neboli $f_1^{-1}xf_1 = f_2^{-1}xf_2$, a tedy podle zavedení f_1, f_2 platí

$$g_1 = f_1^{-1}xf_1 = f_2^{-1}xf_2 = g_2 \,.$$

Platí proto $g_1 = g_2$, a navíc, protože f_i bylo zvoleno libovolně ale pevně pro dané g_i, platí i $f_1 = f_2$. O zobrazení α_{f_i} víme, že je bijekcí, a tedy z $\alpha_{f_i}(h_1) = \alpha_{f_i}(h_2)$ plyne $h_1 = h_1$. Dohromady tedy platí

$$(f_1, h_1) = (f_2, h_2) \,,$$

a tedy zobrazení β_x je injektivní.

Nechť $g \in G$, pak podle věty 2.3.4 platí $g^{-1}xg \in P_x$. Nechť dále f je vybraný prvek množiny $T_{g^{-1}xg}$, pak platí $f \sim_x g$, a tedy podle lemmatu 2.3.2 je $f^{-1}g \in S_x$. Navíc platí

$$\beta((g^{-1}xg, f^{-1}g)) = ff^{-1}g = g \,,$$

a tedy zobrazení β_x je surjektivní. □

Odtud již plyne

$$|P_x \times S_x| = |G| \,.$$

Vzhledem k tomu, že se jedná o direktní součin, platí tedy

$$|S_x| \cdot |P_x| = |G| \,,$$

což potvrzuje platnost veškerých kombinatorických úvah, které byly provedeny v části 2.2.

Poznámka. Sestrojená bijekce rovněž reprezentuje vztah z Lagrangeovy věty, neboť, jak bylo řečeno, třídy rozkladu podle ekvivalence θ_x jsou pravé třídy rozkladu grupy G podle podgrupy S_x, jejichž počet je roven indexu grupy S_x. Podle Lagrangeovy věty platí $|G| = |S_x| \cdot i$, kde i je index podgrupy S_x, tzn. počet tříd rozkladu grupy G podle ekvivalence θ_x, jak bylo dokázáno. Lagrangeova věta sama však nepopisuje vzájemně jednoznačný vztah těchto tříd s prvky množiny P_x.

2.4 Důsledky kombinatorických úvah

Z tvrzení dokázaných v předchozím textu plyne několik zajímavých poznatků o vlastnostech normálních podgrup symetrické grupy G. Tyto důsledky využívají některé speciální typy prvků symetrických grup, které u obecných grup nelze vymezit, neboť pro ně není zaveden pojem stopy prvku.

Věta 2.4.1

Nejmenší normální podgrupa netriviální symetrické grupy G obsahující libovolnou transpozici je celá grupa G.

Důkaz. Nechť $H \trianglelefteq G$ a $t \in H$ je transpozice. Protože H je normální, pak

$$g^{-1}tg \in H$$

pro každé $g \in G$, avšak podle věty 2.3.4 mají permutace $g^{-1}tg$ a t stejnou stopu, a tedy permutace $g^{-1}tg$ jsou rovněž transpozice pro každé $g \in G$. Podgrupa H tak obsahuje všechny transpozice, ale podle věty 1.3.1 je všemi transpozicemi generovaná celá grupa G. $\square$

Uveďme závěrem další podobný důsledek, který platí pro alternující grupu.

Věta 2.4.2

Alternující podgrupa symetrické grupy G všech permutací množiny M ($|M| \geq 3$) je nejmenší normální podgrupa obsahující libovolný 3-cyklus.

Důkaz. Nechť A je normální podgrupa symetrické grupy G a nechť permutace $h \in A$ je 3-cyklus. Protože A je normální, musí obsahovat všechny permutace tvaru $g^{-1}hg$ pro každé $g \in G$. Podle věty 2.3.4 jsou však permutace $g^{-1}hg$ právě všechny 3-cykly, které podle věty 1.3.3 generují alternující podgrupu symetrické grupy G. $\square$

Závěr

Cílem práce bylo studium některých speciálních vlastností permutací konečných množin se zaměřením na jejich skládání. Skládání permutací přitom můžeme chápat jako binární operaci na množině všech permutací a odtud plyne velmi úzké spojení výsledků této práce s teorií grup.

V úvodní kapitole bylo objasněno několik možných vyjádření permutací pomocí skládání permutací jednodušších typů, což přirozeně vedlo k zavedení pojmu stopy, jež je hlavní náplní druhé kapitoly.

Vlastním přínosem této práce je především odlišný přístup k důkazům některých již známých tvrzení a dále také objasnění vztahů plynoucích z teorie grup pomocí kombinatorického aparátu využívajícího vlastností stop permutací. V závěru jsou pak dokázána zajímavá tvrzení o vlastnostech normálních podgrup symetrických grup.

V textu jsme navíc několikrát narazili na možné propojení permutací a mononárních algeber, což také ponechává otevřený prostor vhodný pro další výzkum.

Literatura

[1] Broušek, M.: *O jedné vlastnosti permutací.* Matematika-fyzika-informatika, roč. 22 (2013), č. 2, str. 99-103.

[2] Grillet, P. A.: *Abstract Algebra.* Springer Science + Business Media, LLC, New York 2007.

[3] Hall, M.: *Combinatorial Theory.* Blaisdel, Waltham 1976.

[4] Chajda, I.: *Vybrané kapitoly z algebry.* VUP, Olomouc 2000.

[5] kolektiv autorů: *Kombinatornyj analiz zadači i upražněnija* (rusky). Nauka, Moskva 1982.

[6] Mladenović, P.: *Kombinatorika.* (*Materijali za mlade matematičare, sv. 22*), Društvo matematičara Srbije, Beograd 1992.

[7] Rachůnek, J.: *Grupy a okruhy.* VUP, Olomouc 2005.

[8] Riordan, J.: *An Introduction to Combinatorial Analysis.* John Wiley & Sons, Inc., New York 1958.

[9] Švrček, J.: *Úvod do kombinatoriky.* VUP, Olomouc 2008.