O grupách

5. kapitola. Grupová schémata (tabulky). Isomorfní reprezentace libovolné konečné grupy grupou permutací a grupou matic

In: Ladislav Rieger (author): O grupách. (Czech). Praha: Mladá fronta, 1974. pp. 53–[68].

5. kapitola

GRUPOVÁ SCHÉMATA (TABULKY). ISOMORFNÍ REPREZENTACE LIBOVOLNÉ KONEČNÉ GRUPY GRUPOU PERMUTACÍ A GRUPOU MATIC

Zejména u konečných grup možno se při výzkumu a umělém sestrojování možných typů isomorfie grup (ve shora popsaném smyslu abstraktní teorie grup) opřít o zákonitosti ve čtverečném schématu z prvků grupy, jehož zápisem je grupová tabulka (jak jsme ji poznali již ve 2. kap., která právě dovoluje přehlédnout hotové výsledky grupového násobení bez ohledu na to, jak se k nim došlo. Uveďme si ještě jako čtyři příklady jednoduché grupové tabulky pro všechny grupy řádu 2, 3, 4 (*j* značí vždy jednotkový prvek, ostatní prvky jsou označeny malými latinskými písmeny).

	j	*a*
j	*j*	*a*
a	*a*	*j*

Tab. 2

	j	*a*	*b*
j	*j*	*a*	*b*
a	*a*	*b*	*j*
b	*b*	*j*	*a*

Tab. 3

	j	*a*	*b*	*c*
j	*j*	*a*	*b*	*c*
a	*a*	*b*	*c*	*j*
b	*b*	*c*	*j*	*a*
c	*c*	*j*	*a*	*b*

Tab. 4

	j	*a*	*b*	*c*
j	*j*	*a*	*b*	*c*
a	*a*	*j*	*c*	*b*
b	*b*	*c*	*j*	*a*
c	*c*	*b*	*a*	*j*

Tab. 5

Grupy v tab. 2, 3, 4 jsou tzv. cyklické grupy řádu 2, 3, 4. Obecně cyklickou grupou řádu n rozumíme grupu, jejíž všechny prvky se dají vytvořit mocninami svého vhodného prvku, řekněme a, např. a, $a^2 = j$ v tab. 2; a, $a^2 = b$, $a^3 = j$ v tab. 3; a, $a^2 = b$, $a^3 = c$, $a^4 = j$ v tab. 4. Obecně lze prvky cyklické grupy řádu n vypsat ve tvaru a, a^2, a^3, ..., a^{n-1}, $a^n = j$. (Název „cyklická" grupa pochází z faktu, že mocniny vytvářejícího prvku a se periodicky opakují: $a^{n+1} = a^n \cdot a = j \cdot a = a$, $a^{n+2} = a^2$, ..., což lze znázornit na kružnici.) Číselným případem cyklické grupy řádu n je multiplikativní grupa n-tých odmocnin z 1, což jsou ovšem obecně čísla komplexní.

Tabulka 5 předvádí tzv. Kleinovu grupu; je to komutativní grupa řádu 4, daná např. všemi zákrytovými pohyby obdélníka (nikoli čtverce).

Grupovou tabulku je vhodné zjednodušit tím, že na první místo úvodního řádku i sloupce dáme jednotkový prvek; pak úvodní řádek a úvodní sloupec můžeme vynechat, protože jeden i druhý se opakují v dalším řádku, resp. sloupci.

Jaké vlastnosti takového čtverečného schématu o n^2 polích obsazených n různými věcmi jsou typické pro grupová schémata? Odpověď, kterou podáme v následující větě, dává možnost studovat abstraktní typy isomorfismu konečných grup pomocí jisté konečné kombinatoriky čtverečných uspořádání n různých předmětů.

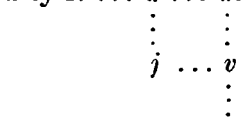
Věta 1

Čtvercové schéma o n^2 polích, zaplněných n různými předměty, j a, b, c, ... — při čemž předmět j nechť leží v levém horním rohu — představuje grupu s jednotkovým prvkem j (v našem smyslu, tj. tak, že za grupový součin xy libovolné-

ho předmětu x s libovolným předmětem y jest třeba pokládat předmět, který je v řádku, uvedeném předmětem x a ve sloupci, uvedeném předmětem y) tehdy a jen tehdy, splňuje-li takové schéma tyto dvě podmínky:

(1) *Každý předmět se vyskytuje v každém řádku a v každém sloupci (a tedy vždy jen jednou).*

(2) *Jestliže sloupec, v němž leží předmět u na místě k-tém shora, se protíná s řádkem, v němž leží předmět v na místě l-tém odleva, v poli obsazeném „jednotkou" j, potom řádek k-tý shora, se protíná se sloupcem l-tým zleva v poli, obsazeném součinem u.v).* (2) je tzv. obdélníkové pravidlo, znázorněné tímto výsekem z tabulky:



Důkaz: Tvrzení má dvě části. Jako první část dokažme, že jestliže předměty j, a, b, ... jsou prvky dané grupy, pak příslušné čtverečné schéma (znázorněné grupovou tabulkou „bez vstupů") má vlastnosti (1) a (2). Jako druhou část dokážeme, že obráceně má-li čtverečné schéma z předmětů j, a, b, ... vlastnosti (1) a (2), pak je tím dána určitá grupa s jednotkovým prvkem j.

Za prvé tedy nechť j je jednotkový prvek a a, b, c, ... ostatní prvky grupy, z nichž je tvořeno čtverečné schéma znázorněné tabulkou.

Vlastnost (1):

Kdyby se jistý prvek grupy, například a, vyskytoval v řádku, uvedeném třeba prvkem b dvakrát, jednou pod prvkem c a jednou pod prvkem d, pak by to znamenalo,

že $b.c = b.d$ $S=$ a. Z toho násobením prvkem b^{-1} zleva by vyplývalo $c = d$. Tedy skutečně nemůže být v témže řádku týž prvek dvakrát.

Vlastnost (2):

Podle předpokladu pro (2) mějme dva prvky u, v v naší grupě, které se vyskytují v příslušném grupovém čtverečném schématu v poloze, vyznačené nejlépe tímto výsekem z tabulky:

	c	...	d	
a	... u	...	ad	...
b	... j	...	v	...

To jest, vycházíme z rovností

$$a.c = u, \quad b.c = j, \quad b.d = v$$

a máme dokázat, že

$$a.d = u.v$$

Z napsaných rovností vyplývá pomocí asociativního zákona a pomocí zákona o inversním prvku

$$a.d = (u.c^{-1})\,(b^{-1}.v) = u(c^{-1}.b^{-1}).v = u.(b.c)^{-1}.v$$
$$= u.j^{-1}.v = u.j.v = u.v$$

protože je

$$(bc)^{-1} = c^{-1}b^{-1}, \text{ t.j. } (bc)\,(c^{-1}b^{-1}) = j$$

Za druhé, nechť čtverečné schéma splňuje podmínky (1) a (2). Máme dokázat, že násobení, zavedené ve smyslu, ve větě uvedeném, splňuje zákony grupy.

Zákon (1) neomezenosti a jednoznačnosti grupového součinu je splněn samozřejmě podle podmínky (1).

Zákon (2) asociativity snadno vyplývá z dvakráte užitého „obdélníkového pravidla", za pomoci tohoto výseku z tabulky:

$$\begin{array}{ccccc} u & \dots & uv & \dots & u(vt) = (uv)\,t \\ \vdots & & \vdots & & \vdots \\ j & \dots & v & \dots & vt \\ & & \vdots & & \vdots \\ & & j & \dots & t \end{array}$$

(Delší a nižší obdélník má v pravém horním rohu součin $u.(v.t)$ kratší a vyšší má na tomtéž místě součin $(u.v).t$; samozřejmě, že tvary obdélníků mohou být různé.)

Zákon (3) jednotkového prvku j je splněn samozřejmě přijatou úmluvou o tom, že první řádek a první sloupec schématu se setkávají v levém horním rohu v místě obsazeném předmětem j (vstupní řádek a vstupní sloupec je nyní nahrazen prvním řádkem a prvním sloupcem vlastní tabulky).

Rovněž konečně i zákon (3) inversního prvku je splněn, třebaže nikoli tak samozřejmě, jak by se snad mohlo zdát.

Abychom to dokázali, zaveďme si na chvíli toto označení: jestliže x je některý z našich n budoucích prvků grupy (tj. z předmětů vystupujících ve zkoumaném schématu), pak jako x_p^{-1} si označíme ten prvek, jímž je uveden sloupec, obsahující jednotkový prvek j v řádku, uvedeném prvkem x. Tento — podle předpokladu (1) — jednoznačně k libovolnému x určený prvek x_p^{-1} bychom mohli nazvat „pravým inversním prvkem" k prvku x, protože splňuje (dle toho, jak byl určen)

rovnost $x.x_p^{-1} = j$ (ve smyslu násobení daného pomocí naší tabulky). Podobně si jako x_L^{-1} označíme prvek, jímž je uvedena řádka, obsahující jednotku ve sloupci, uvedeném pod x. Prvek by mohl být nazván „levým inversním prvkem prvku x", protože splňuje rovnost $x_L^{-1}.x = j$. Nyní, užívajíce již dokázaného asociativního zákona pro naše násobení, máme vynásobením první rovnosti zleva prvkem x_L^{-1} a užitím druhé rovnosti

$$x_L^{-1}.(x.x_p^{-1}) = x_L^{-1}.j = x_L^{-1} = (x_L^{-1}.x).x_p^{-1} = x_p^{-1}$$

Je tedy $x_p^{-1} = x_L^{-1}$. Oba inversní prvky, pravý i levý jsou si rovny, existuje tedy právě jeden inversní prvek x^{-1} ke každému x. Tím je důkaz naší věty dokončen.

Praktické využití této věty k (více méně zkusmému) hledání všech možných typů konečných grup řádu n (při pevném n) sestrojováním tabulek, splňujících podmínky (1) a (2) věty, je velmi omezené: Již pro n, které překročilo 10, je sestavování grupových tabulek zdlouhavé a čím dále méně přehledné, pro náležitě veliké řády by pak nabývaly již samy tabulky (pokud písmena nemají se zmenšovat pod rozměry viditelné okem) nepraktických astronomických velikostí.

Je tedy třeba při studiu všech možných typů isomorfie grup, anebo jak se stručněji, ač méně správně říká, ke studiu abstraktních grup, užít jiných prostředků, totiž hlavně tzv. reprezentace abstraktních grup grupami permutací a grupami matic, o čemž bude řeč v následujícím. (Názvu „abstraktní grupa" možno užívat jen ve smyslu zkratky pro název „typ isomorfismu grup" — „abstraktní" grupy nejsou žádným zvláštním druhem grup.)

K pojmu isomorfní reprezentace abstraktní grupy grupou konkrétní, především grupou matic (jakožto grupou, v níž grupové násobení je dáno pomocí čtyř základních úkonů početních s čísly), jsme vedeni ještě i jinými důvody, z nichž uveďme alespoň tři.

Především všeobecně, jestliže jsme v pojmu typu isomorfismu grup dospěli na (ovšem relativní) vrchol abstrakce, potřebujeme také znát cestu dolů. Poněkud méně obrazně řečeno, jestliže v jistých úvahách teorie grup se nestaráme o to, jak v tom kterém případě se uskutečňuje grupové násobení (v tom či onom typu isomorfie grup), pak při jiných úvahách bychom naopak potřebovali vystihnout (abstraktně pojaté) grupové násobení násobením, které dobře známe z jistého druhu konkrétních grup; při tom musíme ovšem pro toto isomorfní uskutečnění a vystižení čili *reprezentaci* abstraktního grupového násobení konkrétním grupovým násobením zvolit takové reprezentující násobení, které je *univerzální*, aby každé grupové násobení se jím dalo vystihnout a za pomoci isomorfismu nahradit. Takovým univerzálním grupovým násobením je právě *násobení permutací* a ještě lépe: *násobení matic*. (Viz př. 1 a 3 ve **3. kap.**).

Druhým důvodem, který vlastně doplňuje a vysvětluje první, je opora, kterou nám v teorii grup poskytují vztahy mezi čísly, jestliže se nám podaří pomocí isomorfní representace nalézt ke každému typu isomorfismu (konečné nebo i nekonečné grupy, za zvl. předpokladů) grupu matic tohoto typu, jak jsme to například viděli v isomorfním vystižení grupy zákrytových pohybů rovnostranného trojúhelníka a zároveň symetrické grupy S_3 stupně 3 v předchozí kapitole.

Konečně třetí, ovšem nikoli nejméně důležitý důvod k hledání isomorfní reprezentace grup grupami matic,

jsou aplikace fyzikální a jiné, o nichž již byla zmínka.

Než se obrátíme k isomorfním reprezentacím, zaveďme si ještě další, v podstatě známý pojem.

Jestliže část prvků dané grupy tvoří (ve smyslu násobení v dané grupě zavedeného) sama pro sebe grupu, pak této grupě říkáme *podgrupa dané grupy*. Tak všechna celá čísla tvoří podgrupu aditivní grupy všech racionálních čísel (zlomků); tato grupa sama je podgrupou aditivní grupy všech reálných čísel (racionálních a iracionálních dohromady). Všechna čistá otočení, právě tak jako i všechny čisté posuvy tvoří dvě podgrupy v grupě všech euklidovských pohybů roviny. (Všimněme si, že obě podgrupy jsou komutativní, celá grupa však nikoli.) Všechny permutace z n prvních čísel tvoří podgrupu v grupě všech permutací jakéhokoli většího počtu m přirozených čísel.

Věta 2

Ke každé grupě G existuje s ní isomorfní podgrupa G' grupy všech permutací z tolika předmětů, kolik je prvků grupy G (čili jaký je v konečném případě řád n grupy G).

Důkaz: Za permutované předměty vezmeme pro zjednodušení přímo prvky dané grupy G. Samozřejmě že pomocí libovolného očíslování prvků grupy, pokud by jich ovšem byl jen konečný počet, můžeme převést permutace prvků dané grupy v permutace n přirozených čísel, což však již provádět nebudeme.

Ke každému pevnému prvku a z dané grupy G přiřaďme tu permutaci — označme ji π_a, která nahrazuje libovolný prvek x grupy G jeho levým a–násobkem $a.x$, tedy $\pi_a(x) = a.x$. Že π_a je skutečně permutace, je zřejmé, neboť současná náhrada všech prvků x prvky $a.x$ mění dva různé prvky x_1 a x_2 ve dva různé násobky

ax_1 a ax_2, protože by jinak z $a.x_1 = a.x_2$ vyplývalo $x_1 = x_2$ vynásobením prvkem a^{-1} zleva.

Že dvěma různým prvkům grupy a a b jsou takto přiřazeny dvě různé permutace, je rovněž zřejmé, neboť permutace π_a převádí prvek $x = j$ (jednotkový prvek) v prvek a, kdežto permutace π_b převádí týž prvek j v jiný prvek b. Je tedy přiřazení permutace π_a k prvku a grupy vždy vzájemně jednoznačné a zbývá, dle definice 1 ukázat, že součinu prvků je takto přiřazen součin permutací (ve smyslu př. 1, ze 3. kap.) přiřazených daným prvkům. Máme se tedy přesvědčit o platnosti rovnosti

$$\pi_a . \pi_b = \pi_{ab}.$$

Tato rovnost neříká nic jiného, než to, že znásobit libovolný prvek x naší grupy součinem $a.b$ zleva dá totéž, jako znásobit součin $b.x$ zleva prvkem a. To však je právě zaručeno asociativním zákonem. Tím je důkaz věty 2 proveden.

Věta 2 nám tedy zaručuje, že mezi podgrupami symetrické grupy všech permutací (dejme tomu pro konkrétnost) n prvních přirozených čísel nalezneme zástupce všech typů isomorfismu grup řádu n. (Poněvadž jsme však předpokladu konečnosti grupy G nikde v důkazu neužili, platí věta i pro nekonečné grupy, viz 4. kap.). Pozor na to, že symetrická grupa permutací n předmětů, která sama má $n!$ prvků, to jest permutací, může být tedy isomorfně reprezentována podgrupou v symetrické grupě všech permutací z $n!$ předmětů.

Obraťme se k maticím.

Věta 3

Budiž G libovolná grupa (nikoli nutně všech) permutací

z m předmětů (permutací stupně m). Pak existuje v grupě všech regulárních matic stupně m podgrupa isomorfní s danou grupou G.

Důkaz: Permutované předměty si nyní pro jednoduchost nahraďme přirozenými čísly 1, 2, 3, ..., m. (Všechny indexy i, k, l, r, s budou nabývat hodnot od 1 do m.)

Budiž π libovolná permutace z grupy G, která nechť převádí číslo i v číslo $\pi(i)$ (ovšem že $1 \leqq i \leqq m$). Přiřaďme této permutaci π m-řadovou čtverečnou matici, která má v i-tém řádku a v $\pi^{-1}(i)$-tém sloupci (kde π^{-1} je inversní permutace k permutaci π) číslo 1 a na všech ostatních místech má číslo 0, tj. k π přiřazujeme matici (a_{ik}), kde $a_{ik} = 1$ pro $k = \pi^{-1}(i)$ a $a_{ik} = 0$ pro $k \neq \pi^{-1}(i)$. Matice a_{ik} takto přiřazená k permutaci π je jistě regulární, neboť odpovídá lineární homogenní transformaci velmi prostého tvaru

$$\begin{aligned}
X_1 &= 0.X_1' + 0.X_2' + \ldots + 1.X_{\pi^{-1}(1)} + \ldots + 0.X_m' \\
X_2 &= 0.X_1' + 0.X_2' + \ldots + 1.X_{\pi^{-1}(2)} + \ldots + 0.X_m' \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_m &= 0.X_1' + 0.X_2' + \ldots + 1.X_{\pi^{-1}(m)} + \ldots + 0.X_m'
\end{aligned}$$

(Řešení napsaných transformačních rovnic dle čárkovaných neznámých je tím totiž napsáno; je třeba jen převrátit strany rovnic a vhodně přeměnit jejich pořadí; snadno nahlížíme, že lze psát řešení ve tvaru

$$\begin{aligned}
X_1' &= 0.X_1 + 0.X_2 + \ldots + 1.X_{\pi(1)} + \ldots + 0.X_m \\
X_2' &= 0.X_1 + 0.X_2 + \ldots + 1.X_{\pi(2)} + \ldots + 0.X_m \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_m' &= 0.X_1 + 0.X_2 + \ldots + 1.X_{\pi(m)} + \ldots + 0.X_m)
\end{aligned}$$

Protože provedené přiřazení matic k permutacím je zřejmě vzájemně jednoznačné, zbývá jen dokázat, že

součinu dvou permutací $\pi.\varrho$ je přiřazena matice, která je součinem matic, přiřazených k oběma permutacím, a to ve stejném pořadí činitelů. Nechť tedy první permutaci π je přiřazena matice (a_{ik}) s $a_{i\pi^{-1}} = 1$ a $a_{ik} = 0$ pro $k \neq \pi^{-1}(i)$ a podobně permutaci ϱ matice (b_{rs}) s $b_{r\varrho^{-1}} = 1$ a $b_{rs} = 0$ pro $s \neq \varrho^{-1}(r)$ $(i, k, r, s = 1, 2, 3, \ldots, m)$. Znásobením obou matic obdržíme (viz 4. kap.) dle definice

$$(a_{ik}).(b_{rs}) = (c_{is})$$

kde

$$c_{is} = a_{i1}b_{1s} + a_{i2}b_{2s} + \ldots + a_{im}b_{ms}$$

Jasné je, že koeficienty c_{is} matice, která je výsledkem provedeného násobení, budou opět jen čísla 0 nebo 1. Z uvedené definice násobení matic („řádka kráte sloupec") plyne, že bude $c_{is} = 1$ jedině tehdy, když v i-tém řádku matice (a_{ik}) je jednotka na tolikátém místě, na kolikátém (shora) je jednotka v s-tém sloupci matice (b_{rs}). V i-tém řádku matice (a_{ik}) je však vždy jednotka právě na místě $\pi^{-1}(i)$-tém. V s-tém sloupci matice (b_{rs}) je vždy jednotka na právě takovém místě k-tém (shora), že $\varrho^{-1}(k) = s$ čili $k = \varrho(s)$. Tedy k tomu, aby (součet ze součinů) c_{rs} při znásobení r-tého řádku první matice s s-tým sloupcem druhé byl roven 1, je nutno a stačí, aby $\pi^{-1}(r) = k = \varrho(s)$ čili aby $s = \varrho^{-1}\pi^{-1}(r)$. Pak tedy $c_{rs} = 1$ pro $s = \varrho^{-1}\pi^{-1}(r)$ a jinak $c_{rs} = 0$; protože však je $\varrho^{-1}\pi^{-1} = (\pi\varrho)^{-1}$, je tedy $s = (\pi\varrho^{-1}(r)$, takže skutečně obdržená matice c_{rs} je ta, která je přiřazena k permutaci $\pi.\varrho$, čímž je důkaz proveden.

Z věty 2 a 3 plyne ihned

Věta 4

Každá grupa řádu m je isomorfní s jistou grupou matic stupně m (m-řadových matic).

Dle věty 2 lze totiž každou grupu isomorfně reprezentovat vhodnou grupou permutací a dle věty 3 tuto grupu permutací lze opět isomorfně reprezentovat grupou matic; je tím tedy i dána isomorfní reprezentace dané grupy grupou matic.

Věty 3 a 4 mají spíše teoretický, než praktický význam: Zaručují hledanou univerzálnost násobení permutací a násobení matic a dávají nejjednodušší možnost každé grupové násobení v libovolné konečné (a ve vhodném zobecnění i nekonečné) grupě převést v násobení permutací a ještě lépe v násobení matic, to jest v násobení vykonávané pomocí sečítání, odčítání, násobení a dělení čísel. Avšak reprezentace ve smyslu věty 4 vede na matice zbytečně vysokého stupně, totiž rovného řádu grupy. Prakticky, pro studium struktury dané grupy, mají větší význam reprezentace maticemi co nejmenšího stupně (o co nejmenším počtu řádků), kde také větší rozmanitost číselných koeficientů matic a tedy i bohatost jejich vztahů dává více možností využívat aritmetických poznatků pro teorii grup. Prostý příklad takové úsporné a účinné reprezentace grupy zákrytových pohybů rovnostranného trojúhelníka, čili tím i symetrické grupy všech permutací stupně 3 (která je řádu 6), grupami matic stupně 2 jsme si probrali v předchozí kapitole.

V dalším opustíme pojem isomorfní reprezentace, abychom alespoň z dálky ukázali, jakým způsobem řeší abstraktní teorie grup řadu dalších svých typických úkolů. Jde o to, jakým způsobem jednoduché podmínky, kladené na blíže neurčenou grupu, omezují její možný

typ isomorfismu, s cílem stupňovat takové přehledné podmínky tak, až jsou jimi možnosti pro typy isomorfie grupy úplně a přehledně určeny. Poněkud obecněji řečeno, studium logických závislostí jedněch vlastností abstraktní grupy na jiných vlastnostech jiné nebo téže grupy je dalším hlavním úkolem tzv. obecné teorie grup.

Zvláště významný je jmenovitě úkol, na nějž se často v aplikacích teorie grup naráží (např. v aplikacích na teorii algebraických rovnic a na krystalografii), totiž získat co možno úplný přehled o počtu a souvislostech podgrup v grupě, podrobené určitým podmínkám; zvláště pak běží o tzv. normální podgrupy. Abychom mohli alespoň naznačit tyto problémy a jejich řešení, musíme se seznámit s několika dalšími základními, již abstraktními pojmy teorie grup.

Cvičení

1. Ukažte, že grupa je komutativní tehdy a jen tehdy, jestliže její tabulka je souměrná dle hlavní úhlopříčky (zleva nahoře dolů doprava).

2. *Přesvědčte se na podkladě úlohy 1, že všechny grupy řádu menšího než 6 jsou komutativní (Abelovy).

3. *Ukažte, jak je Kleinova grupa isomorfně reprezentována grupou matic

$$j = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

4. Přesvědčte se, že matice daného stupně n takové, že v libovolném řádku a v libovolném sloupci je jediné komplexní číslo různé od nuly — tvoří nekomutativní nekonečnou grupu, tzv. monomiální grupu stupně n. Tato grupa je isomorfní s grupou speciálních tzv. monomiálních (česky: jednočlenných) (lineárních homogenních) transformací tvaru

$$\begin{aligned} x_1' &= k_1 x_{\pi(1)} \\ x_2' &= k_2 x_{\pi(2)} \\ &\dots\dots\dots\dots \\ x_n' &= k_n x_{\pi(n)} \end{aligned}$$

($i = 1, 2, \dots, n$; $\pi(i)$ je permutace hodnot indexu i), $0 \neq k_i$ jsou komplexní čísla.

5. Přesvědčte se, že jestliže koeficienty $k_1, k_2, \dots, k_n$ probíhají pouze čísla z jisté podgrupy multiplikativní grupy komplexních čísel, pak dostaneme monomiální podgrupy monomiální (viz cvič. 4) grupy stupně n. Dokažte, že probíhají-li čísla k_i grupu řádu m, pak taková podgrupa monomiální grupy obsahuje $m^n n!$ prvků (matic).

6. Sestrojte tabulku monomiální (viz cvič. 4) podgrupy stupně 2 pro $k_{1,2} = \pm 1$.

7. Ukažte, že v monomiální (viz cvič. 4) podgrupě stupně 2, kde $k_{1,2}$ probíhají grupu všech 4-tých odmocnin z 1 (t. j. čísla $+1, -1, +i, -i$ ($i = \sqrt{-1}$)) tvoří následující matice podgrupu řádu 8

$$\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \begin{pmatrix} \pm i & 0 \\ 0 & \pm i \end{pmatrix}, \begin{pmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}$$

Ukažte, že v této podgrupě platí tyto vztahy: označíme-li

$$\pm \boldsymbol{i} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}, \pm \boldsymbol{j} = \begin{pmatrix} \pm i & 0 \\ 0 & \mp i \end{pmatrix}, \pm \boldsymbol{k} = \begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix},$$
$$\boldsymbol{l} = \begin{pmatrix} 0 & \pm i \\ \pm i & 0 \end{pmatrix}: \text{ pak je}$$
$$\boldsymbol{i}^2 = \boldsymbol{i}, \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{l}^2 = -\boldsymbol{i}, \boldsymbol{jk} = 1,$$
$$\boldsymbol{kj} = -1, \boldsymbol{kl} = \boldsymbol{j}, \boldsymbol{lh} = -\boldsymbol{j}, \boldsymbol{lj} = \boldsymbol{k}, \boldsymbol{jk} = -\boldsymbol{k}$$

Sestrojte tabulku: $+\boldsymbol{i}, +\boldsymbol{i}, +\boldsymbol{j}, +\boldsymbol{k}$ jsou tzv. základní Hamiltonovy kvaterniony.

8. Ukažte, že multiplikativní grupa všech komplexních čísel o absolutní hodnotě = 1 je isomorfní s grupou všech euklidovských otočení roviny (viz cvič. 1 ke 4 kap.).

9. *Ukažte, že všechny regulární lomené transformace $T(a_1, b_1, a_2, b_2)$ jedné reálné (popř. komplexní) proměnné x tvaru

$$T(a_1, b_1, a_2, b_2) = \left\{ x' = \frac{a_1 x + b_1}{a_2 x + b_2} \right.$$

kde a_1, b_1, a_2, b_2 jsou reálná (komplexní) čísla, tj. parametry transformace $T(a_1, b_1, a_2, b_2)$, která je jimi plně určena, a kde $a_1 b_2 - a_2 b_1 \neq 0$ (podmínka regulárnosti) tvoří grupu (zvláštní případ tzv. projektivní grupy).

Ukažte, že tato grupa (která jakožto grupa transformací jedné proměnné není lineární) je isomorfní s grupou všech lineárních homogenních transformací dvou proměnných (čili je isomorfní s grupou všech regulárních matic stupně 2).

Ukažte, že tzv. afinní transformace tvaru $x' = a_1 x + b_1$ tvoří podgrupu (zvl. případ tzv. afinní grupy).