UNIVERZITA MATEJA BELA V BANSKEJ BYSTRICI
FAKULTA PRÍRODNÝCH VIED
KATEDRA MATEMATIKY

IZOMORFIZMY TORICKÝCH KVOCIENTOV TAPETOVÝCH GRÚP

2009

Jana Majerová
Jarmila Sabová

Poďakovanie

Na začiatku by sme chceli vyjadriť vďaku nášmu konzultantovi Mgr. Ondrejovi Šuchovi, PhD. za odborné, ochotné a najmä trpezlivé vedenie pri našej práci, ako aj za jeho cenné a podnetné rady.

Úvod

Tapetové grupy sú matematickou klasifikáciou rovinných opakujúcich sa vzorov, založenej na symetriách jednotlivých vzorov. Tieto vzory sa často vyskytujú napríklad v architektúre alebo v dekoratívnom umení, ale môžeme ich nájsť aj na bežných veciach, čoho príkladom je dlažba z obrázka (1). Na konci 19-teho storočia klasifikovali matematici E.S. Fedorov, A.M. Schoenflies a W. Barlow vo svojich dielach všetkých 17 tapetových grúp (Fedorov - Symmetry of Crystals).

Torické kvocienty tapetových grúp a ich prezentácie sú spracované v článku Šuch, O.: Vertex-transitive Maps on a Torus, na ktorý sa v našej práci budeme viackrát odvolávať. V tejto práci sme sa zamerali na klasifikáciu izomorfizmov torických kvocientov niektorých tapetových grúp.

Naša práca je rozdelená do šiestich kapitol:

V **kapitolách 1 - 3** sme zhrnuli niektoré poznatky, ktoré sme využívali v ďalších kapitolách. Ide predovšetkým o pojmy konjugácia, akcia grupy na množine, fixované prvky, fixované množiny a ich vlastnosti. Ďalej sme stručne zhrnuli zhodné zobrazenia v rovine, kde sme sa zamerali na ich analytické vyjadrenie a niektoré príklady skladania zhodných zobrazení v rovine.

Kapitola 4 rozpracúva štrukturálne vlastnosti grúp $p1(a,b,c)$ a $p2(a,b,c)$. Pri hľadaní izomorfizmov týchto grúp sme využívali niektoré vlastnosti abelovských grúp, ale aj rády generátorov grúp a počty involúcií.

Kapitola 5 obsahuje štrukturálne vlastnosti grúp $pm_1(a,b)$, $pm_2(a,b)$, $pg_1(a,b)$, $pg_2(a,b)$, $cm_1(a,b)$ a $cm_2(a,b)$. Pri jednotlivých grupách sme využívali všeobecný tvar každého prvku, počty involúcií, veľkosť a štruktúru centra, aby sme vedeli sformulovať tvrdenie, kedy sú grupy navzájom izomorfné.

Kapitola 6 obsahuje grupy $pmm_1(a,b)$, $pmm_2(a,b)$, $pmg_1(a,b)$, $pmg_2(a,b)$, $pgg_1(a,b)$ a $pgg_2(a,b)$ a ich štrukturálne vlastnosti. Podobne ako v predchádzajúcej kapitole aj tu sme využívali predovšetkým počty involúcií a všoebecný tvar každého prvku grupy. V tejto kapitole pri niektorých grupách sme využili aj kolmosť prvkov v grupe, aby sme našli podmienky, kedy sú grupy izomorfné.

V **závere** rozpracúvame niektoré ďalšie izomorfizmy, na ktoré sme pri analyzovaní jednotlivých grúp narazili. Jedná sa predovšetkým o abelovské grupy. Keďže sme pre nedostatok času nemohli spracovať všetky izomorfizmy medzi jednotlivými kvocientami, pridali sme ich do záveru ako načrtnutie ďalších otázok týkajúcich sa tapetových grúp.

Obrázok 1: Ukážky použitia vzorov, ktoré tapetové grupy vytvárajú.

Na predchádzajúcich obrázkoch môžeme vidieť, že tapetové grupy sa dajú nájsť na rôznych veciach. Na prvom obrázku je dlažba z Budapešti, na nej nachádzame grupu *pgg*. Posunuté zrkadlenia sa v tomto prípade nachádzajú na diagonále. Druhý obrázok znázorňuje misu z Kermy, na ktorej môžeme objaviť *pmg*. Ďalším príkladom nádoby, na ktorej sa nachádza vzor vygenerovaný niektorou tapetovou grupou je bronzová misa z Asýrie, ktorej vzor sa nachádza na treťom obrázku. V nej nájdeme grupu *cm*. Našli by sa ešte ďalšie príklady, kto má záujem, na intenete sa ich nachádza skutočne obrovské množstvo.

Obsah

Zoznam obrázkov

1 Konjugácia

Definícia 1.1 *Nech G je grupa. Pre každé $g \in G$ definujme zobrazenie $\gamma_x : G \to G$, dané predpisom $x \longmapsto gxg^{-1}$, kde $x \in G$. Potom takéto zobrazenie γ_x nazývame* konjugáciou prvkom g.

Hovoríme, že prvok $y \in G$ je *konjugovaným prvkom* k prvku $x \in G$ práve vtedy, keď existuje také $g \in G$ pre ktoré platí $gxg^{-1} = y$.
Konjugácia je reláciou ekvivalencie v grupe, pretože je

- reflexívna, $exe^{-1} = x$,
- symetrická, lebo ak $gxg^{-1} = y$, potom $g^{-1}yg = x$
- tranzitívna, lebo ak $gxg^{-1} = y$ a $hyh^{-1} = z$, potom
  $(hg)x(hg)^{-1} = hgxg^{-1}h^{-1} = h(gxg^{-1})h^{-1} = hyh^{-1} = z$.

Množinu prvkov konjugovaných s prvkom x voláme *trieda konjugácie* prvku x.

2 Fixované prvky

Základným pojmom, s ktorým budeme pracovať v tejto kapitole je pojem *akcie grupy na množine.*

Definícia 2.1 *Nech X je ľubovolná množina a nech G je grupa, v ktorej násobenie jej prvkov značíme $\cdot$. Povieme, že grupa G* má na množine X akciu, *ak pre každý prvok (g, x) z množiny $G \times X$ je definovaný prvok $g * x$, spĺňajúci nasledujúce podmienky:*

- $e * x = x$
- $g * (h * x) = (g \cdot h) * x$.

Príklad 2.1 *Ak $X = G$, potom G má prirodzenú akciu*

- *násobenia a platí* $g * x = g.x$
  $e * x = e.x = x$
  $g * (h * x) = g.(h.x) = (g.h).x$
- *konjugácie prvkom g a platí* $g * x = g.x.g^{-1}$
  $e * x = e.x.e^{-1} = x$
  $g * (h * x) = g * (h.x.h^{-1}) = g.h.x.h^{-1}.g^{-1} = (g.h).x.(g.h)^{-1}$

Ale G nemá prirodzenú akciu konjugácie prvkom g^{-1}, pretože pre $g * x = g^{-1}.x.g$ neplatí
$g * (h * x) = (g \cdot h) * x$.
$e * x = e^{-1}.x.e = x$
$g * (h * x) = g * (h^{-1}.x.h) = g^{-1}.h^{-1}.x.h.g = (h.g)^{-1}.x.(h.g)$

Pre zjednodušenie zápisu budeme operáciu $*$ vynechávať.

Definícia 2.2 *Nech $g \in G$, $x \in X$ a G je grupa s akciou na množine X. Povieme, že prvok x je fixovaný prvkom g, ak $gx = x$.*

Príklad 2.2 *Príklady fixovaných prvkov:*

- *Ak $g = e$, tak všetky prvky sú fixované.*
- *Jediný prvok, ktorý je fixovaný otočením, je stred otočenia.*
- *Posunutie nemá žiadny fixovaný bod.*

Definícia 2.3 *Nech G je grupa s akciou na množine X. Povieme, že množina $A \subseteq X$ je fixovaná prvkom $g \in G$, ak pre každý prvok $a \in A$ platí $ga \in A$.*

Veta 2.1 *Nech grupa G má akciu na množine X. Ak $x \in X$ je fixovaný prvkom $g \in G$, tak prvok hx je fixovaný prvkom hgh^{-1}, kde $h \in G$.*

Dôkaz: Počítajme akciu prvku hgh^{-1} na prvok hx.

$$hgh^{-1}(hx) =$$

z druhej vlastnosti akcie na množine dostávame

$$= (hgh^{-1}h)x$$

z asociatívnosti násobenia v grupe dostávame

$$= (hg(h^{-1}h))x$$

v grupe platí $h^{-1}h = e$, tak dostávame

$$= (hg)x$$

z druhej vlastnosti akcie na množine dostávame

$$= h(gx)$$

podľa predpokladu, že x je fixovaný prvkom g, nakoniec dostaneme

$$= hx.$$

čbtd

Veta 2.2 *Nech grupa G má akciu na množine X. Ak množina $A \subseteq X$ je fixovaná prvkom $g \in G$, potom hA je fixovaná množina prvkom hgh^{-1}, kde $h \in G$.*

Dôkaz: dokazovať budeme priamo podobne ako v predchádzajúcej vete: pre každý prvok $a \in A$ dostaneme
$hgh^{-1}(ha) = (hgh^{-1}h)a = (hg(h^{-1}))a = (hg)a = h(ga) = ha.$
čbtd

3 Prehľad zhodných zobrazení v rovine

V tejto časti uvedieme stručný prehľad zhodných zobrazení v rovine a aj niektoré príklady skladania zhodných zobrazení v rovine, ktoré budeme využívať v ďalších kapitolách.

Zhodné zobrazenia sa dajú popísať niekoľkými spôsobmi. Analyticky ich môžeme vždy zapísať v tvare:

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \mathbf{A} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix},$$

kde $\mathbf{A}$ je matica typu 2×2 s determinantom ± 1. Ak identifikujeme dvojrozmerný priestor s komplexnými číslami $z = x + yi$, tak zobrazenia s $\det \mathbf{A} = 1$ sa dajú zapísať v tvare

$$z \mapsto az + b,$$

kde a je komplexné číslo s absolútnou hodnotou 1. Zobrazenia s $\det \mathbf{A} = -1$ sa dajú zapísať v tvare

$$z \mapsto a\bar{z} + b,$$

kde a je komplexné číslo s absolútnou hodnotou 1.

3.1 Identické zobrazenie

Identické zobrazenie alebo *identita* je zobrazenie, ktoré priraďuje prvku množiny ten istý prvok rovnakej množiny. Identitu môžeme zapísať ako zobrazenie $Id : R^2 \to R^2$, pre ktoré platí

$$Id : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x \\ y \end{pmatrix}$$

pre každý prvok $\begin{pmatrix} x \\ y \end{pmatrix} \in R^2$.

3.2 Osová súmernosť

Osová súmernosť alebo *reflexia* s osou o je také zobrazenie, ktoré každý bod A ležiaci na osi o zobrazí sám na seba a každý bod A ležiaci mimo osi o zobrazí na bod A' tak, že priamka o je osou súmernosti úsečky AA'. Reflexia je sama sebe inverzným zobrazením, pretože zložením dvoch reflexií s rovnakou osou dostaneme identitu. Čiže reflexia je involúciou. Ak si za os súmernosti zvolíme priamku $x = 0$, tak reflexiu zapíšeme ako zobrazenie $O : R^2 \to R^2$, pre ktoré platí

$$O : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x \\ -y \end{pmatrix}$$

3.3 Posunutie

Posunutie alebo *translácia* je také zobrazenie, ktoré každý bod A posunie v rovnakom smere a o rovnakú vzdialenosť na bod A'. Teda smer a veľkosť posunutia sú charakterizované *vektorom posunutia* a tým je posunutie určené jednoznačne.
Transláciu môžeme zapísať ako zobrazenie $T : R^2 \to R^2$, pre ktoré platí

$$T : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

3.4 Otočenie

Otočenie alebo *rotácia* je zhodné zobrazenie určené bodom (stredom otočenia) a uhlom otočenia, ktorý je nenulový. Analyticky môžeme rotáciu zapísať ako zobrazenie $R : R^2 \to R^2$, pre ktoré platí

$$R : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

Stredová súmernosť je špeciálnym prípadom otočenia o 180 stupňov.

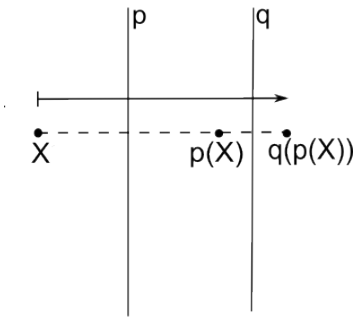
3.5 Posunutá súmernosť

Posunutá súmernosť alebo *posunuté zrkadlenie* je zobrazenie, ktoré vznikne zložením reflexie a posunutia. Posunuté zrkadlenie môžeme zapísať ako zobrazenie $P : R^2 \to R^2$, pre ktoré platí

$$P = P_1 \circ P_2$$

$$P_1 : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} b_1 \\ 0 \end{pmatrix}$$

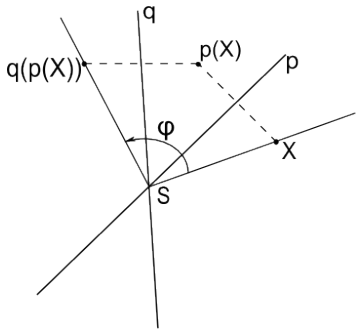
$$P_2 : \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} x \\ -y \end{pmatrix}$$



Obrázok 2: Zloženie dvoch reflexií s rovnobežnými osami $(q \circ p)(X)$

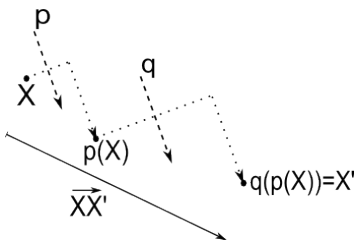
3.6 Niektoré príklady skladania zhodných zobrazení

- Zložením dvoch reflexií s rovnakou osou dostaneme identitu
- Zložením dvoch reflexií s rôznymi rovnobežnými osami dostaneme posunutie, ktorého dĺžka sa rovná dvojnásobku vzdialenosti osí reflexií
- Zložením dvoch rôznobežných reflexií p a q dostaneme otočenie, kde priesečník osí súmernosti je stred otočenia. Ak skladáme reflexie predpisom $(q \circ p)(X) = q(p(X))$, tak veľkosť orientovaného uhla otočenia φ podľa obrázka (3) sa rovná dvojnásobku veľkosti ostrého uhla, ktorý zvierajú dané reflexie. Ak skladáme reflexie predpisom $(p \circ q)(X)$, tak veľkosť orientovaného uhla sa rovná dvojnásobku veľkosti tupého uhla, ktorý zvierajú reflexie p a q.



Obrázok 3: Zloženie dvoch rôznobežných reflexií $(q \circ p)(X)$

- Zložením dvoch posunutí dostávame posunutie
- Zložením dvoch otočení s rovnakým stredom získame otočenie s tým istým stredom otočenia
- Zložením dvoch posunutých zrkadlení, ktoré majú rovnobežné osi súmernosti, dostaneme posunutie (nezáleží na orientácii vektorov posunutia)



Obrázok 4: Zloženie dvoch posunutých zrkadlení $(q \circ p)(X)$

4 Grupy $p1$, $p2$

4.1 Štrukturálne vlastnosti grupy $p1(a, b, c)$

Grupa $p1(a, b; c)$ je definovaná nasledujúcou prezentáciou

$$p1(a, b; c) := \langle X, Y | [X, Y] = X^a = Y^b X^c = 1 \rangle . \tag{1}$$

Z relácie $[X, Y] = 1$ plynie, že jej generátory komutujú, a teda grupa $p1(a, b, c)$ je vždy abelovská. Pre štruktúru abelovských grúp platí nasledujúca všeobecná veta:

Veta 4.1 *Každá konečná abelovská grupa s k generátormi je izomorfná grupe*

$$Z_{d_1} \times Z_{d_2} \times ... \times Z_{d_k}$$

kde platí

$$d_1 | d_2 | ... | d_k.$$

Na dôkaz tejto vety si uvedieme dve vety bez dôkazu (dôkaz nájdete v knihe $[II.]$). Budeme používať označenie $G(p)$, čo je podgrupa abelovskej grupy, do ktorej patria všetky tie prvky, ktorých rád je mocninou prvočísla p. Ďalej použijeme pojem p - grupy, čo je grupa, ktorej rádom je mocnina prvočísla p. Používame aj pojem postupnosti typu $(p^{r_1}, ..., p^{r_s})$, čo je grupa $Z_{p^{r_1}} \times ... \times Z_{p^{r_s}}$.

Veta 4.2 *Nech G je konečná abelovská grupa. Potom G je súčin grúp $G(p)$, kde p je prvočíslo.*

Veta 4.3 *Každá konečná abelovská p - grupa je izomorfná súčinu cyklických p - grúp. Ak je to postupnosť typu $(p^{r_1}, ..., p^{r_s})$, kde*

$$1 \leq r_1 \leq r_2 \leq ... \leq r_s,$$

potom je táto postupnosť jednoznačne daná.

Na dôkaz vety 4.1 ešte musíme dokázať nasledujúce dve lemy.

Lema 4.1 *Podgrupa $G(p)$ konečnej abelovskej grupy G je p - grupou.*

Dôkaz: Aby $G(p)$ bola p - grupou, musí platiť $Order(G(p)) = p^k$. Nech rád $Order(G(p)) = np^k$, kde p a n sú nesúdeliteľné. Keďže je G abelovská, potom je komutatívna aj $G(p)$, potom súčin rádov jednotlivých jej generátorov musí byť násobkom veľkosti grupy $G(p)$. Ale, rády generátorov sú mocniny prvočísla p, potom aj súčin bude mocninou prvočísla p a ten delí znovu len mocnina prvočísla p, čiže $n = 1$.
čbtd

Nasledujúca lema nám hovorí, koľko generátorov majú niektoré z podgrúp ľubovoľnej grupy G.

Lema 4.2 *Nech konečnú grupu G generuje k generátorov a N je jej ľubovoľná normálna podgrupa, potom grupu G/N generuje maximálne k generátorov.*

Dôkaz: Vezmime si krátku exaktnú postupnosť $1 \xrightarrow{\varphi} N \xrightarrow{\psi} G \xrightarrow{\tau} G/N \xrightarrow{\lambda} 1$. Potom τ bude surjektívnym homomorfizmom. Nech $g_1, ..., g_k$ sú generátory grupy G, potom každý prvok $g \in G$ je konečnou postupnosťou týchto generátorov. Nech $g = g_1^{n_1^1}...g_k^{n_k^1} g_1^{n_1^2}...g_k^{n_k^m}$, potom ale $\tau(g) = \tau(g_1^{n_1^1}...g_k^{n_k^1} g_1^{n_1^2}...g_k^{n_k^m}) = \tau(g_1)^{n_1^1}...\tau(g_k)^{n_k^m}$. Keďže je τ surjektívne zobrazenie, potom pre každý prvok $h \in G/N$ existuje také $g \in G$, že platí $\tau(g) = h$, potom ale každé h je generované maximálne k prvkami.
čbtd

Ďalšia lema hovorí o tom, aké veľké musí byť s z vety 4.3.

Lema 4.3 *Nech abelovskú grupu G generuje k prvkov. Nech pre prvočíslo p je $G(p)$ určená postupnosťou typu $(p^{r_1}, p^{r_2}, ..., p^{r_s})$, potom platí $s \leq k$.*

Dôkaz: Najprv musíme dokázať, že postupnosť typu $(p^{r_1}, p^{r_2}, ..., p^{r_s})$, ktorá je izomorfná p - grupe $G(p)$, generuje práve s prvkov.

Nech ju generuje viac prvkov, nech je to počet m, teda platí $s < m$. Označme prvok $e_1 = (1, 0, ...0), e_2 = (0, 1, 0, ..., 0), ...$, teda e_i bude taký vektor, ktorý bude mať na i - tom mieste číslo 1, na ostatných miestach budú 0. Prvkov e_i je v tomto prípade s. Pomocou nich ale vygenerujeme každý prvok $G(p)$, potom aj prvky postupnosti typu $(p^{r_1}, p^{r_2}, ..., p^{r_s})$.

To, že ju generuje minimálne s prvkov, dokážeme matematickou indukciou vzhľadom na s.

Nech $s = 1$, potom grupa $Z_{p^{r_1}}$ je generovaná 1 prvkom, teda tvrdenie platí.

Nech tvrdenie platí pre $s = n$, dokážeme, že platí aj pre $s = n + 1$.
Majme postupnosť typu $(p^{r_1}, p^{r_2}, ..., p^{r_n}, p^{r_{n+1}})$. Vzhľadom na to, že je to abelovská grupa, môžeme predpokladať, že $r_1 \leq r_2 \leq ... \leq r_n \leq r_{n+1}$. Nech $r_n < r_{n+1}$. Grupa $K := Z_{p^{r_1}} \times Z_{p^{r_2}} \times ... \times Z_{p^{r_n}} \times Z_{p^{r_{n+1}}}$ obsahuje ako svoju podgrupu grupu $H := Z_{p^{r_1}} \times Z_{p^{r_2}} \times ... \times Z_{p^{r_n}}$. Z indukčného predpokladu generuje túto grupu minimálne n prvkov. Exponentom tejto podgrupy je zrejme číslo p^{r_n}. Prvok e_{n+1} má ale rád $p^{r_{n+1}} > p^{r_n}$, preto ho nemôžu generovať prvky z podgrupy H. Nech ale patrí nejaká mocnina prvku e_{n+1} do grupy H, potom má poslednú zložku nulovú, čo platí len pre mocninu p^{n+1}, potom grupa H má s grupou $\langle e_{n+1} \rangle$ triviálny prienik. Teda, grupa má minimálne $n + 1 = s$ generátorov.

Teraz predpokladajme, že $r_n = r_{n+1}$. Nech grupu K generuje menej ako s prvkov, nech ju generuje maximálne m prvkov, kde $m < s$. Potom z indukčného predpokladu existuje taká grupa izomorfná grupe K, ktorá bude izomorfná postupnosti typu $(p^{l_1}, p^{l_1}, ..., p^{l_m})$, ktorá má minimálne m generátorov. Potom ale pre p - grupu $G(p)$ existujú dve postupnosti (typu $(p^{l_1}, p^{l_1}, ..., p^{l_m})$ a typu $(p^{r_1}, p^{r_2}, ..., p^{r_n}, p^{r_{n+1}})$), čo je v spore s vetou 4.3, teda aj túto grupu generuje minimálne $n + 1 = s$ prvkov.

Keďže sme dokázali, že grupu $G(p)$ generuje maximálne s a minimálne s prvkov, musí ju generovať práve s prvkov.

Nech $G \cong G(p_1) \times ... \times G(p_r)$, potom je zrejme grupa $N = G(p_1) \times ... \times G(p_{i-1}) \times G(p_{i+1}) \times ... \times G(p_r)$ normálnou podgrupou grupy G pre každé $i \in \{1, 2, ..., r\}$. Potom ale podľa predchádzajúcej lemy grupu $G/N = G(p_i)$ generuje maximálne k prvkov. Teda, použitím predchádzajúceho platí $s \leq k$.
čbtd

Teraz už môžeme dokázať vetu zo začiatku tejto sekcie.

Dôkaz: Majme konečnú abelovskú grupu G. Nech jej rád je číslo $p1^{m_1}...pl^{m_l}$, kde p_i sú prvočísla a $m_i \in \{0, 1, ...\}$, potom táto grupa je izomorfná súčinu $G(p_1) \times G(p_2) \times ...G(p_l)$.

Podľa vety 4.3 pre každú podgrupu $G(p_i)$ existuje jednoznačná postupnosť typu $(p^{r_1}, ..., p^{r_n})$. Potom grupa G je izomorfná grupe

$$G \cong Z_{{p_1}^{r(1)_1}} \times ... \times Z_{{p_1}^{r(1)_{n_1}}} \times ... \times Z_{{p_l}^{r(l)_1}} \times ... \times Z_{{p_l}^{r(l)_{n_l}}}. \quad (2)$$

Ak grupa G má k generátorov, potom podľa predchádzajúcej lemy je číslo $n_i \leq k$ pre každé $i \leq l$. Ak $n_i < k$, potom vytvoríme novú postupnosť typu $(0, ..., r(i)_1, ..., r(i)_{n_i})$, tú preznačíme na $(r(i)_1, ..., r(i)_k)$. Ak niektoré $r(i)_j$ je nulové, potom $Z_{p^i_{r(i)_j}} \cong Z_1$ a pre každé Z_r bude platiť $Z_1 \times Z_r \cong Z_r$.

Keďže je G abelovská, potom je taktiež izomorfná grupe
$Z_{p_1^{r(1)_1}} \times Z_{p_2^{r(2)_1}} \times ... \times Z_{p_l^{r(l)_1}} \times ... \times Z_{p_1^{r(1)_k}} \times ... \times Z_{p_l^{r(l)_k}}$. Vzhľadom na to, že jednotlivé p_i sú s p_j nesúdeliteľné pre $i \neq j$, potom platí

$$Z_{p_1^{r(1)_i}} \times Z_{p_2^{r(2)_i}} \times ... \times Z_{p_l^{r(l)_i}} \cong Z_{p_1^{r(1)_i} p_2^{r(2)_i} ... p_l^{r(l)_i}}.$$

Označme si $p_1^{r(1)_i} p_2^{r(2)_i} ... p_l^{r(l)_i} = d_i$. Potom grupa $G \cong Z_{d_1} \times Z_{d_2} \times ... Z_{d_k}$, kde platí $d_1|d_2|...|d_k$.
čbtd

Aby sme mohli použiť túto vetu, treba určiť exponent grupy $p1(a,b;c)$. Keďže exponent *abelovskej* grupy je najmenším spoločným násobkom rádov, generátorov, v našom prípade stačí určiť rády prvkov X a Y. Na určenie rádu prvku Y budeme potrebovať jednu vetu z teórie čísel.

Veta 4.4 *Diofantická rovnica $ax + by = c$ má riešenie práve vtedy, ak $gcd(a,b)|c$.*

Dôkaz: Nech rovnica $ax + by = c$ má riešenie, ukážeme, že $gcd(a,b)|c$. Nech $a = gcd(a,b)a'$ a $b = gcd(a,b)b'$, potom $ax + by = gcd(a,b)a'x + gcd(a,b)b'y = gcd(a,b)(a'x + b'y) = c$. Keďže číslo $gcd(a,b)$ delí ľavú stranu rovnosti, potom musí deliť aj číslo c.

Nech $c = gcd(a,b).c'$ a nech $ka + lb = gcd(a,b)$. Prenásobme túto rovnicu číslom c', dostávame $a(kc') + b(lc') = gcd(a,b).c' = c$, potom $x = kc'$ a $y = lc'$.
čbtd

Teraz už môžeme dokázať vetu o rádoch generátorov grupy $p1(a,b;c)$.

Veta 4.5 *Nech X, Y sú generátory grupy $p1(a,b,c)$ danej prezentáciou (1). Potom*

a) rád prvku X je a,

b) rád prvku Y je $\dfrac{ab}{gcd(a,c)}$.

Dôkaz: Z prezentácie (1) plynie, že rád prvku X delí a. Avšak z geometrickej realizácie ukázanej na obrázku (5) plynie, že rád prvku X je aspoň a. Tým sme dokázali časť a).

Na výpočet rádu prvku použijeme vzťah:

$$Order(H.G) = \frac{Order(H \times G)}{Order(H \cap G)}. \tag{3}$$

Vzhľadom na to, že $p1(a,b;c)$ je abelovská grupa, bude množina
$\langle X \rangle . \langle Y \rangle := \left\{ X^i Y^j, 0 \leq i < Order(X), 0 \leq j < Order(Y) \right\}$ nosičom grupy $p1(a,b;c)$. Jeho veľkosť je podľa článku [*I.*] ab. V predchádzajúcej časti tohto dôkazu sme si ukázali, že rád prvku X je a.

Teraz ukážeme, že grupou $\langle X \rangle \cap \langle Y \rangle$ je podgrupa $\left\langle X^{gcd(a,c)} \right\rangle$. Z prezentácie (1) vieme, že $X^a = X^c Y^b = 1$. Chceme zistiť, pre ktoré m bude existovať také celé číslo n, aby platilo: $X^m = Y^n$ a teda $X^m Y^{-n} = 1$. Keďže sa pohybujeme v abelovskej grupe, môžeme prehlásiť jednotlivé prvky $X^j Y^k$ za vektory (j,k). Ak $(a,0) = (c,b) = (0,0)$, potom aj $k(a,0) + l(c,b) = (0,0) = (m,-n)(1)$. Našou úlohou je nájsť také m, aby rovnosť (1) platila. Máme vyriešiť rovnicu $ka + lc = m$. Vo vete 4.4 sme si dokázali, že takáto rovnica má riešenie jedine vtedy, keď $gcd(a,c)|m$. Teda, do podgrupy $\langle X \rangle \cap \langle Y \rangle$ patria len prvky $X^{r.gcd(a,c)}$.

Potom po dosadení dostávame:

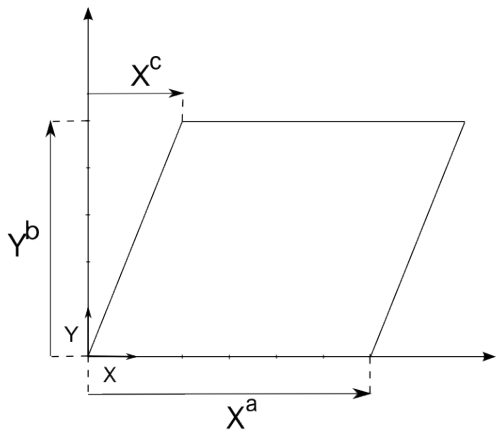
$$ab = \frac{a.Order(Y)}{Order(H \cap G)} = \frac{a.Order(Y)}{Order(\left\langle X^{gcd(a,c)} \right\rangle)} = \frac{a.Order(Y)}{\frac{Order(X)}{gcd(gcd(a,c),Order(X))}} =$$

$$= \frac{a.Order(Y)}{\frac{a}{gcd(gcd(a,c),a)}} = \frac{a.Order(Y)}{\frac{a}{gcd(a,c)}} = Order(Y).gcd(a,c),$$

čiže

$$Order(Y) = \frac{ab}{gcd(a,c)}.$$

čbtd



Obrázok 5: Grupa $p1(a,b,c)$

Veta 4.6 *Grupa* $p1(a,b;c)$ *je izomorfná grupe*

$$Z_{\frac{ab}{gcd(a,b,c)}} \times Z_{gcd(a,b,c)}$$

Dôkaz: Vďaka tomu, že $p1(a,b;c)$ je abelovská grupa, stačí nám vedieť exponent, ktorým je najmenší spoločný deliteľ rádov jej generátorov.

$$lcm(a, \frac{ab}{gcd(a,c)}) = \frac{a.a.b}{gcd(a,c).gcd(a, \frac{ab}{gcd(a,c)})}$$

tu využívame fakt $lcm(a,b) = \frac{a.b}{gcd(a,b)}$

$$= \frac{a.a.b}{gcd(a.gcd(a,c), a.b)}$$

kde sme využili, že $gcd(cx,cy) = c.gcd(x,y)$

$$= \frac{a.a.b}{a.gcd(gcd(a,c),b)}$$
$$= \frac{a.b}{gcd(gcd(a,c),b)}$$
$$= \frac{a.b}{gcd(a,b,c)}$$

v tomto bode sme využili asociativitu a komutatatívnosť operácie gcd.
čbtd

Počet involúcií v grupe $p1(a,b;c)$ automaticky plynie z toho, že je izomorfná súčinu dvoch cyklických grúp.

Dôsledok 4.1 *Grupa* $p1(a,b,c)$ *má*

- *žiadnu involúciu, ak a a b sú nepárne čísla,*
- 1 *involúciu, ak a alebo b je párne, ale* $gcd(a,b,c)$ *je nepárne,*
- 3 *involúcie, ak* a,b,c *sú párne čísla.*

Všetky vety použité v tejto podkapitole smerovali k nájdeniu rôznych tried neizomorfných grúp. Kedy sú dve grupy $p1(a,b;c)$ a $p1(a',b';c')$ izomorfné, hovorí nasledujúca veta.

Veta 4.7 *Grupy $p1(a,b;c)$ a $p1(a',b';c')$ sú izomorfné práve vtedy, ak $ab = a'b'$ a zároveň $gcd(a,b,c) = gcd(a',b',c')$.*

Na dôkaz tejto vety budeme potrebovať dokázať nasledujúcu, všeobecnú vetu o izomorfizmoch grupy $Z_m \times Z_n$ spolu so $Z_{m'} \times Z_{n'}$.

Veta 4.8 *Grupy $Z_m \times Z_n$ a $Z_{m'} \times Z_{n'}$ sú izomorfné práve vtedy, keď $mn = m'n'$ a $gcd(m,n) = gcd(m',n')$.*

Dôkaz:
(„⇒")
Nech $Z_m \times Z_n$ je izomorfná so $Z_{m'} \times Z_{n'}$. Potom, keďže sú izomorfné, ich rády sa rovnajú, teda $mn = m'n'$. Musíme ešte dokázať $gcd(m,n) = gcd(m',n')$.

Najväčším rádom v grupe $Z_m \times Z_n$ je číslo $lcm(m,n)$. Nech existuje väčší rád. Potom existuje prvok (k,l) taký, že $lcm(m,n).(k,l) \neq (0,0)$. Ale $m|lcm(m,n)$ a teda aj $m|lcm(m,n).k$ a podobne $n|l.gcd(m,n)$, čo je spor s predpokladom, že existuje väčší rád ako $lcm(m,n)$. Nech je najväčším rádom číslo $k < lcm(m,n)$. Potom bude platiť $k.(1,1) = (0,0)$. Keďže $k < lcm(m,n)$, potom platí buď k nedelí m alebo k nedelí n. Čo je spor s tým, že $(k,k) = (0,0)$. Teda, najväčším rádom v grupe $Z_m \times Z_n$ je číslo $lcm(m,n)$. V grupe $Z_{m'} \times Z_{n'}$ je najväčším rádom číslo $lcm(m',n')$. Tieto dve čísla sa musia rovnať a po jednoduchej úprave a po využití rovnosti rádov grúp dostávame $gcd(m,n) = gcd(m',n')$.

(„⇐")
Nech $mn = m'n'$ a $gcd(m,n) = gcd(m',n')$. Dokážeme, že obe grupy ($Z_m \times Z_n$ a $Z_{m'} \times Z_{n'}$) sú izomorfné rovnakej grupe. Tou grupou bude $Z_{gcd(m,n)} \times Z_{lcm(m,n)}$.

Grupa $Z_m \times Z_n$ je konečná abelovská grupa, ktorú generujú prvky $(1,0)$ a $(0,1)$, kde $Order((1,0)) = m$ a $Order((0,1)) = n$. Z vety 4.1 vieme, že grupa $Z_m \times Z_n$ je izomorfná grupe $Z_{d_1} \times Z_{d_2}$. Číslo d_2 je exponent, čo je najmenší spoločnú násobok $lcm(m,n)$, potom $d_1 = \frac{ab}{lcm(m,n)} = gcd(m,n)$. Týmto sme ukázali, že grupa $Z_m \times Z_n \cong Z_{gcd(m,n)} \times Z_{lcm(m,n)}$. Analogicky sa ukáže $Z_{m'} \times Z_{n'}$.
čbtd

Teraz už môžeme dokázať vetu 4.7.

Dôkaz: Grupa $p1(a,b;c) \cong Z_{gcd(a,b,c)} \times Z_{\frac{ab}{gcd(a,b,c)}}$ a $p1(a',b';c') \cong Z_{gcd(a',b',c')} \times Z_{\frac{a'b'}{gcd(a',b',c')}}$.

(„⇒")
Nech sú uvedené grupy izomorfné. Potom podľa vety 4.8 musí platiť:
$gcd(a,b,c).\frac{ab}{gcd(a,b,c)} = gcd(a',b',c').\frac{a'b'}{gcd(a',b',c')}$, čo po jednoduchých úpravách znamená, že $ab = a'b'$. Ešte máme dokázať $gcd(a,b,c) = gcd(a',b',c')$. Z izomorfizmu daných dvoch grúp a z predchádzajúcej vety ďalej vyplýva nasledujúca rovnosť: $gcd\left(gcd(a,b,c), \frac{ab}{gcd(a,b,c)}\right) = gcd\left(gcd(a',b',c'), \frac{ab}{gcd(a',b',c')}\right)$. Vzhľadom na to, že $(gcd(a,b,c))^2|ab$ (resp. $(gcd(a',b',c'))^2|ab$), potom $gcd\left(gcd(a,b,c), \frac{ab}{gcd(a,b,c)}\right) = gcd(a,b,c)$ (resp. $gcd\left(gcd(a',b',c'), \frac{ab}{gcd(a',b',c')}\right) = gcd(a',b',c')$). Čím sme dokázali aj rovnosť najväčších spoločných deliteľov.

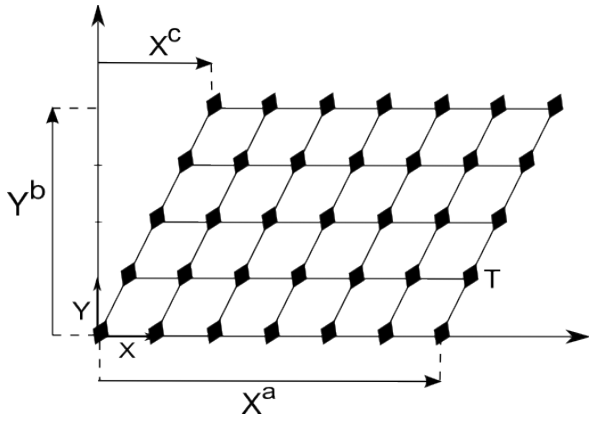
(„⇐")
Nech $ab = a'b'$ a $gcd(a,b,c) = gcd(a',b',c')$. Potom sú obe grupy izomorfné rovnakej grupe, a to $Z_{gcd(a,b,c)} \times Z_{\frac{ab}{gcd(a,b,c)}}$.
čbtd

4.2 Štrukturálne vlastnosti grupy $p2(a,b;c)$

Grupa $p2(a,b;c)$ je grupa, ktorú generujú dve posunutia a involutórna rotácia. Existuje viac ekvivalentných definícií tejto grupy a jednou z nich je:

$$p2(a,b;c) = \langle T, X, Y | [X,Y] = T^2 = (TX)^2 = (TY)^2 = X^a = Y^b X^c = 1 \rangle . \tag{4}$$

Geometrickú prezentáciu tejto grupy znázorňuje obrázok (6)



Obrázok 6: Grupa $p2(a,b;c)$

Podgrupou $p2(a,b;c)$ je grupa $\langle X, Y | [X,Y] = X^a = Y^b X^c = 1 \rangle$, čo je ale prezentácia grupy $p1(a,b;c)$. Vzhľadom na to, že veľkosť grupy $p1(a,b;c)$ je ab a veľkosť grupy $p2(a,b;c)$ je $2ab$ (vyplýva z článku [*I.*]), má táto podgrupa index 2 a keďže každá podgrupa indexu 2 je normálna, potom platí $p1(a,b;c) \triangleleft p2(a,b;c)$. Môžeme teda grupu $p2(a,b;c)$ vyjadriť nasledujúcim spôsobom: $p2(a,b;c) = p1(a,b;c) \cup T.p1(a,b;c) = \langle T \rangle .p1(a,b;c)$.

Veta 4.9 *Grupy $p2(a,b;c)$ a $p2(a',b';c')$ sú izomorfné práve vtedy, ak sú izomorfné grupy $p1(a,b;c)$ s $p1(a',b';c')$.*

Pred jej dôkazom si ale uvedieme ešte jeden príklad, z ktorého vzíde počet involúcií v grupe $p2(a,b;c)$ triviálne.

Príklad 4.1 Majme prvok grupy $p2(a,b;c)$, ktorý je tvaru TX^iY^j, kde X^iY^j je ľubovoľný prvok grupy $p1(a,b;c)$. Pre každý takýto prvok platí, že je rádu 2. Teda,
$TX^iY^jTX^iY^j = TX^iY^jTY^jX^i = TX^iY^{j-1} \underbrace{YTY}_{\text{z prezentácie } YTY = XTX = T} Y^{j-1}X^i = ... = TX^iTX^i =$
$TT = 1$. Potom v grupe $p2(a,b;c)$ bude $ab + n$, kde n je počet involúcií v grupe $p1(a,b;c)$.

Teraz si dokážeme vetu 4.9.

Dôkaz:
(„⇒")
Nech sú grupy $p2(a,b;c)$ a $p2(a',b';c')$ izomorfné. Máme dokázať, že potom sú aj grupy $p1(a,b;c)$ s $p1(a',b';c')$ izomorfné. Z vety 4.7 vieme, že dve grupy $p1(a,b;c)$ a $p1(a',b';c')$ sú izomorfné práve vtedy, ak $ab = a'b'$ a $gcd(a,b,c) = gcd(a',b',c')$. Vzhľadom na to, že veľkosť grupy $p2(a,b;c)$ je $2ab$ a to sa musí rovnať veľkosti grupy $p2(a',b';c')$, čo je $2a'b'$, potom dostávame prvú z podmienok izomorfnosti triviálne.

V predchádzajúcom príklade sme si dokázali, že každý prvok z množiny $T.p1(a,b;c)$ je rádu 2. Teda, prvok najväčšieho rádu pochádza z podgrupy $p1(a,b;c)$, resp. $p1(a',b';c')$ (momentálne vynechávame možnosť, že sa jedná o grupu $p2(1,1;c)$). V prvom prípade je tým rádom číslo $\frac{ab}{gcd(a,b,c)}$, v druhom $\frac{a'b'}{gcd(a',b',c')}$. Z predpokladu sú grupy $p2(a,b;c)$ a $p2(a',b';c')$ izomorfné, potom sa musia aj

najväčšie rády rovnať a využitím rovnosti $ab = a'b'$ dostávame $gcd(a,b,c) = gcd(a',b',c')$, čím sme dokázali túto časť vety.

Majme grupu $p2(1,1;c)$, aby bola s grupou $p2(a',b';c')$ izomorfná, musí $a' = 1$ a $b' = 1$. Potom v oboch prípadoch sú podgrupy $p1(1,1;c)$ a $p1(1,1;c')$ triviálne a teda sú izomorfné.

(„⇐")
Nech sú grupy $p1(a,b;c)$ a $p1(a',b';c')$ izomorfné. Potom existuje nejaké zobrazenie dané predpisom:

$$\varphi : p1(a,b;c) \longrightarrow p1(a',b';c').$$

Rozšírme toto zobrazenie na $\varphi*$, ktoré bude prvky grupy $p1(a,b;c)$ zobrazovať na prvky grupy $p1(a',b';c')$ rovnako ako φ a involúciu T zobrazí na involúciu T'.

Ukážeme, že je to homomorfizmus. V podgrupe $p1(a',b';c')$ spĺňa $\varphi*$ všetky relácie vyplývajúce z prezentácie, keďže φ je izomorfizmus. Prvok TX^kY^j zobrazí $\varphi*$ na $T'\varphi(X^kY^j)$. Nech $\varphi(X^kY^j) = X'$ a $\varphi(X^mY^n) = Y'$. V príklade 4.1 sme si ukázali, že každý prvok z množiny $T.p1(a,b;c)$(resp. $T', p1(a',b';c')$) je involúcia. Potom $\varphi*(1) = \varphi*((TX^kY^j)^2) = \varphi*(TX^kY^j)^2 = (T'X')^2 = 1$, podobne aj $\varphi*((TX^mY^n)^2) = 1$.

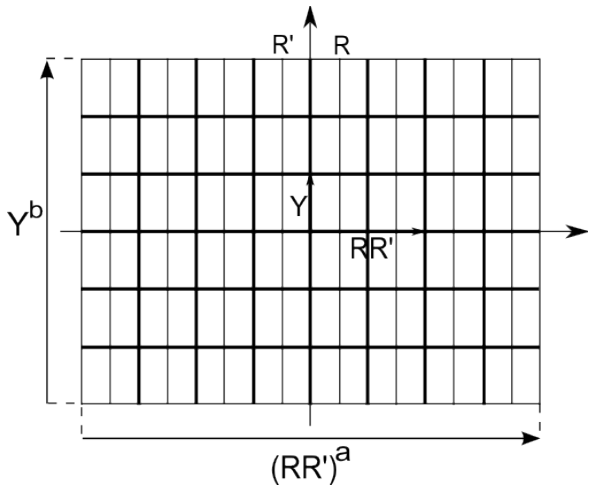
Keďže $\varphi*$ je homomorfizmus a platí $\varphi*(T) = T', \varphi*(X^kY^j) = X'$ a $\varphi*(X^mY^n) = Y'$, potom grupou $Im(\varphi*)$ bude celá grupa $p2(a',b';c')$ a $\varphi*$ bude surjektívne zobrazenie. Keďže $p1(a,b;c)$ a $p1(a',b';c')$ sú izomorfné, platí $ab = a'b'$, potom majú grupy $p2(a,b;c)$ a $p2(a',b';c')$ rovnaké rády a zobrazenie $\varphi*$ musí byť aj injektívne.
čbtd

5 Grupy pm, pg, cm

5.1 Štrukturálne vlastnosti grupy $pm_1(a,b)$

Grupa $pm_1(a,b)$ je grupa, ktorú generujú 2 reflexie a 1 posunutie. Predstavu, ako táto grupa vyzerá nám dáva obrázok (7) a jej štrukturálne vlastnosti budeme skúmať z prezentácie:

$$pm_1(a,b) := \left\langle R, R', Y | [R,Y] = [R',Y] = R^2 = R'^2 = (RR')^a = Y^b = 1 \right\rangle . \tag{5}$$



Obrázok 7: Grupa $pm_1(a,b)$

Nasledujúca veta nám hovorí, akej všeobecnej grupe je $pm_1(a,b)$ izomorfná. Vďaka nej dostávame dôsledky, na základe ktorých vieme vylúčiť izomorfizmy medzi jednotlivými grupami $pm_1(a,b)$ a $pm_1(a',b')$.

Veta 5.1 *Grupa $pm_1(a,b)$ daná prezentáciou (5) je izomorfná grupe*

$$Z_b \times D_{2a}.$$

Dôkaz: Musíme dokázať, že v grupe $pm_1(a,b)$ existujú normálne podgrupy izomorfné Z_b a D_{2a}, pre ktoré platí

$$Z_b \cap D_{2a} = \{1\} . \tag{6}$$

Grupa $\langle Y \rangle$ je cyklická podgrupa centra grupy $pm_1(a,b)$. Z prezentácie (5) vieme, že rád prvku Y delí číslo b. Z obrázku (7) ale vidíme, že rád musí byť aspoň b. Potom $\langle Y \rangle \cong Z_b$.

Nech je podgrupa H daná prezentáciou

$$H := \left\langle R, RR' | R^2 = (RR')^a = (R(RR'))^2 = 1 \right\rangle$$

Podgrupa H obsahuje všetky slová z písmen R a R', keďže R je jedným z generátorov tejto podgrupy a $R' = R(RR')$. Podľa definície je táto podgrupa grupy $pm_1(a,b)$ dihedrálna. Aby sme ukázali, že je aj normálna, musíme ukázať, že pre všetky prvky patriace do $pm_1(a,b)$ platí:

$$g.H = H.g$$

Všetky slová skladajúce sa len z R a R' však túto podmienku spĺňajú, keďže pre $g \in H$ je $g.H = H = H.g$, teda musíme overiť podmienku pre slová tvaru $Y^i.h$ (tu využívame to, že každá mocnina prvku

Y komutuje so všetkými prvkami grupy $pm_1(a,b)$, teda prvky tvaru $Y^{i_1}.h_1.Y^{i_2}h_2...Y^{i_n}.h_n$ môžeme písať v tvare $Y^{i_1+i_2+...+i_n}.h_1.h_2...h_n = Y^i.h$, kde $h_1.h_2...h_n = h$ a $i_1 + i_2 + ...i_n \equiv i \pmod b$), kde $h \in H$. Iné prvky už grupa $pm_1(a,b)$ neobsahuje (nemá už iné generátory). Prvok Y^i patrí do centra a teda podmienku (6) spĺňa (keďže $Y^i.h.H = Y^i.H = H.Y^i = H.h.Y^i = H.Y^i.h$). Teda pogrupa H je normálna.

Stačí už len ukázať, že predchádzajúce dve podgrupy majú len jednotkový prienik. Keďže mocniny prvku Y komutujú s každým prvkom podgrupy H, v ktorej sa nachádzajú všetky slová skladajúce sa z prvkov R a R', potom vzhľadom na to, že grupa $pm_1(a,b)$ iné generátory nemá, bude platiť $pm_1(a,b) = \langle Y \rangle .H$. Z článku [*I.*] vieme, že $Order(pm_1(a,b)) = 2ab$, ďalej využijúc vzťah (3) dostávame, že $Order(\langle Y \rangle \cap H) = \{e\}$.
čbtd

Jedným z priamych dôsledkov predchádzajúcej vety je počet involúcií, ktorý bude hlavným nástrojom pri vete o izomorfizmoch.

Dôsledok 5.1 *Grupa $pm_1(a,b)$ má*

- *a involúcií, ak a je nepárne a b je nepárne,*
- *$a+1$ involúcií, ak a je párne a b nepárne,*
- *$2a+1$ involúcií, ak a je nepárne a b je párne a*
- *$2a+3$ involúcií, ak a aj b sú párne.*

Veta 5.2 *Grupy $pm_1(a,b)$ a $pm_1(a',b')$ sú izomorfné práve vtedy, ak platí $ab = a'b'$ a zároveň:*

a) $a = a'$ *a* $b = b'$,

b) $(a,b) = (\frac{a'}{2}, 2b')$ *alebo* $(a,b) = (2a', \frac{b'}{2})$, *vtedy ak* $a + b \equiv a + a' \equiv b + b' \equiv 1 \pmod 2$.

Dôkaz:
(„⇒")

I. Nech sú a aj b nepárne. Potom, keďže sú podľa predpokladu grupy izomorfné, musia sa ich rády rovnať, teda platí rovnosť $ab = a'b'$. Keďže 2 nedelí ab, potom musia byť aj a' a b' nepárne. Z rovnosti počtu involúcií dostávame rovnicu $a = a'$, potom aj $b = b'$.

II. Nech je a párne a b nepárne. Grupa $pm_1(a,b)$ má v tomto prípade $a+1$ involúcií.

   a) Nech a' je párne a b' nepárne. Pri izomorfizme sa musia počty involúcií rovnať, potom $a = a'$.

   b) Nech a' je nepárne a b' párne. Potom z rovnosti involúcií dostávame $a + 1 = 2a' + 1$, teda $a' = \frac{a}{2}$ a $b' = 2b$.

   c) Nech sú a' aj b' párne. Počet involúcií v grupe $pm_1(a',b')$ je potom $2a' + 3$. Po dosadení do rovnosti $a = 2a' + 2$. Z poslednej rovnosti vyplýva, že štvorka a nedelí, ale keďže delí súčin $a'b' = ab$ a b je nepárne, potom musí deliť a.

III. Nech a je nepárne a b párne.

   d) Nech a' je párne a b' nepárne. Bude existovať inverzné zobrazenie z $pm_1(a',b')$ do $pm_1(a,b)$, ktorého podmienky sme prešetrili v bode $II.b$), čiže $a' = 2a$ a $b' = \frac{b}{2}$.

   e) Nech a' je nepárne a b' párne. Z rovnosti počtu involúcií dostávame $a = a'$, potom aj $b = b'$.

f) Nech sú a' aj b' párne. Takýto prípad nastať nemôže, pretože ak $4|a'b = ab$ a zároveň $gcd(a,2) = 1$, potom musí platiť $4|b$. Z rovnosti počtu involúcií vyplýva, že $a = a' + 1$, potom $b = \frac{ab}{a-1}$. Nech $ab = 2^j k$ a $a - 1 = 2^i l$, kde $gcd(2,k) = gcd(2,l) = 1$, potom $b = 2^{j-i}\frac{k}{l}$, potom ale $ab = 2^{j-i}\frac{k}{l}(2^i l + 1)$, keďže číslo $(2^i l + 1)\frac{k}{l}$ dvojka nedelí, potom pre nenulové i prichádzame do sporu s deliteľnosťou ab číslom 2^j a pre nulové i bude číslo a rovné $l + 1$, čo vzhľadom na to, že l je nepárne, je spor s predpokladom, že a je nepárne. Nech $l = 0$, potom $a' = 0$, čo je v spore s rádom grupy.

IV. Nech sú a aj b párne.

g) Nech $a' + b' \equiv 1 \pmod 2$, potom sme nemožnosť inverzného izomorfizmu dokázali v bodoch $II.c)$ a $III.f)$.

h) Nech sú a' aj b' párne. Potom z rovnosti počtu involúcií $a = a'$, potom aj $b = b'$.

(„⇐")
Nech $(a,b) = (a',b')$, potom grupy $pm_1(a,b)$ a $pm_1(a',b')$ izomorfné sú.
Nech a je párne a b nepárne a $a' = \frac{a}{2}$ je nepárne a nech $b' = 2b$. Vezmime zobrazenie:

$$\begin{aligned} \varphi : pm_1(a,b) &\longmapsto pm_1(a',b') \\ \varphi : R &\longmapsto R^\star Y^{\star b} \\ \varphi : R' &\longmapsto R'^\star \\ \varphi : Y &\longmapsto Y^{\star b+1}. \end{aligned}$$

Aby sme ukázali, že to je homomorfizmus, musíme ukázať, že platí $\varphi(R)^2 = \varphi(R')^2 = \varphi(RR')^a = \varphi(Y)^b = 1$ a $\varphi(R)\varphi(Y) = \varphi(Y)\varphi(R)$ a $\varphi(R')\varphi(Y) = \varphi(Y)\varphi(R')$.

$$\begin{aligned} \varphi(1) = \varphi(R^2) = \varphi(R)^2 = R^{\star 2}Y^{\star 2b} = 1.Y^{\star b'} = 1 \\ = \varphi(R'^2) = \varphi(R')^2 = R'^{\star 2} = 1 \\ = \varphi((RR')^a) = \varphi(RR')^a = (\varphi(R)\varphi(R'))^a = (R^\star Y^{\star b} R'^\star)^a = (Y^{\star b}(R^\star R'^\star))^a = \\ = (Y^{\star 2b})^{\frac{a}{2}}((R^\star R'^\star)^{\frac{a}{2}})^2 = (Y^{\star b'})^{\frac{a}{2}}((R^\star R'^\star)^{a'})^2 = 1 \\ = \varphi(Y^b) = \varphi(Y)^b = (Y^{\star b+1})^b = (Y^{\star 2b})^{\frac{b+1}{2}} = (Y^{\star b'})^{\frac{b+1}{2}} = 1 \end{aligned}$$

$$\begin{aligned} \varphi(R)\varphi(Y) = R^\star Y^{\star b} Y^{\star b+1} = Y^{\star b+1} R^\star Y^{\star b} = \varphi(Y)\varphi(R) \\ \varphi(R')\varphi(Y) = R'^\star Y^{\star b+1} = Y^{\star b+1} R'^\star = \varphi(Y)\varphi(R'). \end{aligned}$$

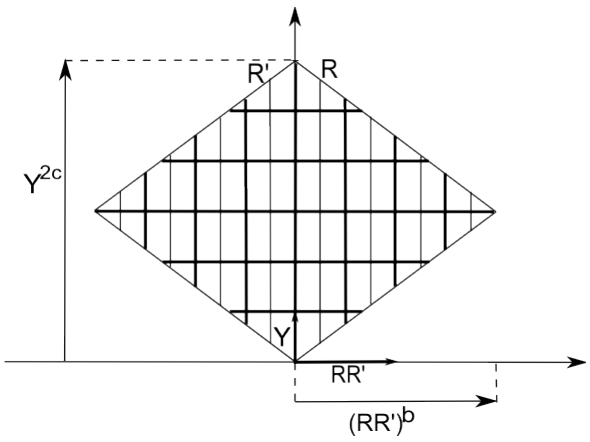
Teraz ukážeme, že je to izomorfizmus. Množina $\{R, R', Y\}$ generuje grupu $pm_1(a,b)$. Keďže $Im(\varphi)$ je podgrupou, potom do nej patrí aj prvok $(Y^{\star b} R^\star R'^\star)^{\frac{a}{2}} = Y^{\star b.\frac{a}{2}}(R^\star R'^\star)^{\frac{a}{2}} = Y^{\star b}$. Posledná rovnosť platí, pretože $\frac{a}{2} = a'$ a to je nepárne číslo a rád prvku $Y^\star$ je $2b$. Ale potom tam patrí aj prvok $Y^{\star -b}$ a teda aj $R^\star Y^{\star b} Y^{\star -b} = R^\star$. Do podgrupy $Im(\varphi)$ patrí ale aj prvok $Y^{\star b+1} Y^{\star -b} = Y^\star$. Generujúcou množinou podgrupy $Im(\varphi)$ je potom $\left\{R^\star, R'^\star, Y^\star\right\}$, táto množina ale generuje celú grupu $pm_1(a',b')$ a teda φ je surjektívne zobrazenie. Keďže $ab = \frac{a}{2}.2b$, potom aj rovnosť rádov platí a grupy $pm_1(a,b)$ a $pm_1(a',b')$ sú izomorfné.

Nech a je nepárne a b je párne a nech $a' = 2a$ a $b' = \frac{b}{2}$ je nepárne. Potom hľadaným izomorfizmom bude zobrazenie φ^{-1}.
čbtd

5.2 Štrukturálne vlastnosti grupy $pm_2(b,c)$

Ďalšou štruktúrou v tapetových grupách je grupa $pm_2(b,c)$ daná prezentáciou:

$$pm_2(b,c) := \left\langle Y, R, R' | R^2 = R'^2 = (RR')^b Y^c = Y^{2c} = RYRY^{-1} = R'YR'Y^{-1} = 1 \right\rangle. \qquad (7)$$



Obrázok 8: Grupa $pm_2(b,c)$

Ako si takú grupu môžeme geometricky predstaviť, nám udáva obrázok (8)
Úlohou tejto kapitolky je dokázať nasledujúcu vetu.

Veta 5.3 *Ak $(b,c) \neq (b',c')$, tak grupy $pm_2(b,c)$ a $pm_2(b',c')$ nie sú izomorfné.*

Na dôkaz tejto vety musíme najprv ukázať nasledujúce tri vety. Najprv si ukážeme jednu vetu z teórie čísel, ktorú budeme používať vo viacerých dôkazoch v tomto článku.

Veta 5.4 *Pre každú dvojicu celých čísel p a q, kde $q \neq 0$ existuje dvojica celých čísel r,s taká, že platí:*

$$p = qs + r \qquad 0 \leq r < |q|. \tag{8}$$

Táto dvojica je jednoznačne určená.

Dôkaz: Nech $q > 0$, potom $q \geq 1$. Vezmime si všetky celočíselné násobky čísla q. Potom existuje nejaké číslo s také, že $sq \leq p$ (také číslo určite existuje, napríklad $s = -|p|$). Potom platí $r = p - sq \geq 0$ a r je prirodzené číslo. Vytvorme si z čísel r množinu M. Keďže je M podmnožinou prirodzených čísel, bude existovať najmenší prvok r. Nech platí $r \geq q$, potom $0 \leq r - q = p - sq - q = p - (s+1)q = r'$, kde $r = r' + q \geq r'$, čo je spor s predpokladom, že r je najmenšie číslo z množiny M.

Nech existujú aspoň dve dvojice r_1, s_1 a r_2, s_2 také, že platí $s_1 q + r_1 = s_2 q + r_2 = p$. Potom $0 = q(s_1 - s_2) + (r_1 - r_2)$, čiže $(s_2 - s_1)q = r_1 - r_2$, kde $-q < r_1 - r_2 < q$. Ľavú stranu číslo q delí, ale pravú len v prípade, že $r_1 - r_2 = 0$, potom $r_1 = r_2$ a zároveň $s_1 = s_2$.

Nech $q < 0$, potom $-q > 0$ a podľa predchádzajúcej časti existuje jedinečná dvojica r a s taká, že $p = s(-q) + r$, kde $0 \leq r < -q$, potom $p = (-s)q + r$.
čbtd

Nasledujúca veta nám hovorí, ako vyzerá každý prvok v grupe $pm_2(b,c)$.

Veta 5.5 *Každý prvok grupy $pm_2(b,c)$ je jednoznačne daný tvarom $Y^i X^j R^k$, kde $i \in \{0,1,...,2c-1\}$, $j \in \{0,1,...,b-1\}$, $k \in \{0,1\}$ a $X = RR'$.*

Dôkaz: Keďže grupa $pm_2(b,c)$ je generovaná iba prvkami Y, R, R', potom každá konečná postupnosť, ktorej členy patria do množiny $\{Y, R, R'\}$ určuje v grupe $pm_2(b,c)$ nejaký prvok. Z prezentácie (7) vyplýva, že prvok Y komutuje s prvkom R aj R', teda v našej postupnosti môžme všetky Y „presunúť" na začiatok. Nech je prvkov Y v postupnosti i'. Za nimi sa nachádza podpostupnosť tvorená len prvkami R a R'. Keďže rád oboch prvkov je 2, potom uvažujeme len nasledujúce dva prípady:

a) $Y^{i'}(RR')^{j'}R^k$, kde $k \in \{0,1\}$ a $0 \leq j'$

b) $Y^{i'}(R'R)^{j'}R'^{k}$, kde $k \in \{0,1\}$ a $0 \leq j'$.

Majme prípad a). V predpokladoch vety je, že prvok $X = RR'$, teda dostávame, že daný prvok je tvaru $Y^{i'}X^{j'}R^{k}$. Z prezentácie (7) vyplýva, že $X^{b} = Y^{-c} = Y^{c}$. Podľa vety 5.4 existuje taká dvojica celých čísel q, j, že $j' = qb + j$, kde $0 \leq j < b$. Teda $X^{j'} = X^{qb+j} = X^{qb}X^{j} = (X^{b})^{q}X^{j} = Y^{cq}X^{j}$. Po dosadení dostávame $Y^{i'}X^{j'}R^{k} = Y^{i'+cq}X^{j}R^{k}$. Ďalej nám z prezentácie plynie, že rád prvku Y delí $2c$, a teda z tohto predpokladu a opätovným využitím vety 5.4 dostávame $Y^{i'+cq} = Y^{p2c+i} = (Y^{2c})^{p}Y^{i} = 1^{p}Y^{i} = Y^{i}$. Po konečnej úprave: $Y^{i'+cq}X^{j}R^{k} = Y^{i}X^{j}R^{k}$, kde $0 \leq i < 2c, 0 \leq j < b, 0 \leq k < 2$, čo je požadovaného tvaru.

Majme prípad b). Keďže $X = RR'$, potom $X^{-1} = (RR')^{-1} = R'^{-1}R^{-1} = R'R$, a teda $(R'R)^{j'} = X^{-j'}$. Z konečnosti grupy $pm_2(b,c)$ vyplýva aj konečnosť rádu prvku X a teda z prezentácie (7) vyplýva, že $X^{-j'} = X^{2b-j'} = (RR')^{2b-j'}$. Teda $Y^{i'}(R'R)^{j'}R'^{k} = Y^{i'}X^{2b-j'-k}R^{k}R'^{k}R'^{k} = Y^{i'}X^{2b-j'-k}R^{k}$, ďalej postupujeme rovnako ako v bode a), čím opäť dostávame požadovaný tvar.

Ešte nám ostáva dokázať jednoznačnosť daného tvaru. Z článku [*I.*] ale vieme, že rád grupy $pm_2(b,c)$ je $4bc$, čo je ale počet rôznych kombinácií exponentov i, j, k.
čbtd

Ak si uvedomíme, že prvkami grupy $pm_2(b,c)$ sú zobrazenia, nebude už nasledujúcu vetu ťažké dokázať.

Veta 5.6 *Centrum grupy $pm_2(b,c)$ je*

- *cyklická grupa generovaná prvkom Y, ak $b \neq 1$ a*
- *celá grupa, ak $b = 1$.*

Dôkaz: V predošlej vete sme dokázali, že každý prvok je tvaru $Y^{i}X^{j}R^{k}$. Bez ujmy na všeobecnosti môžeme definovať zobrazenia Y, R, R', X nasledovne.

$$Y : (u,v) \longmapsto (u,v) + (0,1) \tag{9}$$

$$R : (u,v) \longmapsto (-u,v) \tag{10}$$

$$R' : (u,v) \longmapsto (-u,v) + (1,0) \tag{11}$$

$$X = RR' : (u,v) \longmapsto (u,v) - (1,0) \tag{12}$$

V predchádzajúcich riadkoch sme predpokladali, že reflexia R je daná osou súmernosti $x = 0$ a R' je daná osou $x = \frac{1}{2}$. Teda

$$Y^{i}X^{j}R^{k} : (u,v) \longmapsto ((-1)^{k}u, v) - (j,0) + (0,i) \tag{13}$$

Centrum ľubovoľnej grupy je definované ako množina prvkov, ktoré komutujú s každým prvkom grupy. Teda, ak prvok $Y^{i}X^{j}R^{k}$ patrí do centra, potom musí platiť nasledujúca rovnosť:

$$Y^{i}X^{j}R^{k}Y^{i'}X^{j'}R^{k'}(u,v) = Y^{i'}X^{j'}R^{k'}Y^{i}X^{j}R^{k}(u,v),$$

kde i, j, k sú pevne dané a i', j', k' sú ľubovoľné a bod (u,v) je tiež ľubovoľný. Keďže prvok Y komutuje s každým prvkom dostávame rovnosť: $Y^{i}X^{j}R^{k}Y^{i'}X^{j'}R^{k'} = Y^{i+i'}X^{j}R^{k}X^{j'}R^{k'}$ a podobne $Y^{i'}X^{j'}R^{k'}Y^{i}X^{j}R^{k} = Y^{i+i'}X^{j'}R^{k'}X^{j}R^{k}$. Využitím (9), (10), (11), (12) a (13) dostávame:

$$Y^{i+i'}X^{j}R^{k}X^{j'}R^{k'} : (u,v) \longmapsto ((-1)^{k+k'}u - (-1)^{k}j' - j, b + i + i')$$

$$Y^{i+i'}X^{j'}R^{k'}X^{j}R^{k} : (u,v) \longmapsto ((-1)^{k+k'}u - (-1)^{k'}j - j', b + i + i')$$

Teda:

$$((-1)^{k+k'}u - (-1)^{k}j' - j, b + i + i') = ((-1)^{k+k'}u - (-1)^{k'}j - j', b + i + i')$$

$$(-1)^{k+k'}u-(-1)^{k}j'-j=(-1)^{k+k'}u-(-1)^{k'}j-j'$$
$$b+i+i'=b+i+i'$$

Posledná rovnosť platí pre ľubovoľné i a i'. Druhá rovnosť musí platiť pre všetky k', teda aj pre $k'=0$. Po dosadení dostávame

$$-(-1)^{k}j'-j=-j-j'$$
$$(-1)^{k}j'=j'.$$

Nech $b\neq 1$, potom j' môže nadobúdať aj nenulové hodnoty. Keďže táto rovnosť platí pre každé j', potom musí platiť : $k=0$. Ak $b=1$, potom $j'=0$ a rovnosť platí pre každé k. Ale rovnosť platí aj pre $k'=1$. Teda

$$-j'-j=j-j'$$
$$2j=0$$
$$j=0.$$

Z predošlých rovností dostávame, že pre $b\neq 1$ patria do centra prvky $Y^iX^0R^0=Y^i$, kde $i\in\{0,1,...,2c-1\}$. Z čoho vyplýva, že centrum tvoria iba všetky mocniny prvku Y, a teda centrum je cyklická grupa generovaná prvkom Y. Pre $b=1$ sú v centre Y^iR^k, čo je spolu $4c$ prvkov, to je ale veľkosť grupy $pm_2(b,c)$, teda grupa je abelovská.
čbtd

Teraz už môžme dokázať vetu zo začiatku tejto sekcie.
Dôkaz: Keďže veľkosť grupy $pm_2(b,c)$ je $4bc$, musí byť aj veľkosť grupy $pm_2(b',c')$ rovnaká, teda $4bc$, čo vyplýva priamo z vlastností izomorfizmov. Lenže veľkosť centra prvej grupy pre $b\neq 1$ je $2c$, čo celá grupa nie je, potom ani druhá grupa abelovská nie je a veľkosť centra druhej grupy je $2c'$. Ak sú grupy $pm_2(b,c)$ a $pm_2(b',c')$ izomorfné, potom musia mať centrum rovnakej veľkosti a teda $2c=2c'$, z čoho už priamo plynie $(b,c)=(b',c')$. Ak $b=1$, potom je grupa $pm_2(b,c)$ abelovská, potom musí byť komutatívna aj $pm_2(b',c')$, či znamená $b'=1$ a potom $c'=c$.
čbtd

5.3 Štrukturálne vlastnosti grupy $pg_1(a,b)$

Grupa pg_1 je generovaná dvoma posunutými zrkadleniami. Zapísať jej prezentáciu môžme nasledovne:

$$pg_1(a,b):=\left\langle P,Q|P^2=Q^2,(P^{-1}Q)^a=P^{2b}=1\right\rangle. \tag{14}$$

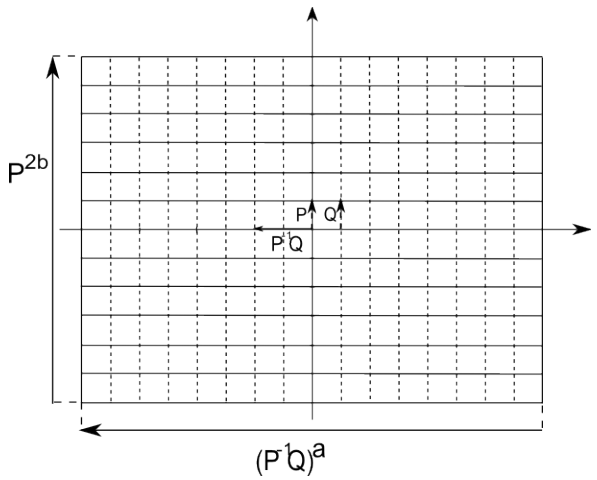
Postupovať budeme rovnako ako pri predchádzajúcej grupe, t.j. najprv určíme kanonický tvar prvku.

Veta 5.7 *Každý prvok grupy $pg_1(a,b)$ sa dá jednoznačne vyjadriť tvarom:*

$$(P^2)^k(P^{-1}Q)^jP^l, \text{kde } 0\leq k<b,\ 0\leq j<a,\ 0\leq l<2. \tag{15}$$

Dôkaz: Túto vetu dokážeme analogicky ako vetu o štruktúre prvkov grupy $pm_2(a,b)$. Každý prvok našej grupy je konečná postupnosť jej generátorov. Keďže z prezentácie (14) vieme, že $P^2=Q^2$, potom $P^2Q=Q^2Q=Q^3=QQ^2=QP^2$, teda P^2 komutuje s prvkom Q a teda aj s každým prvkom grupy a môžme ho presunúť na začiatok postupnosti. Nech je v celej postupnosti k_1 prvkov P^2. Potom dostávame napríklad postupnosť tvaru: $(P^2)^{k_1}PQP\underbrace{QQ}_{P^2}QPQPQQPQPQPQQQ....$ Nech je prvkov Q^2 v postupnosti k' - krát. Označme si $k_2=k_1+k'$. Teda dostávame postupnosti tvaru:

a) $(P^2)^{k_2}(PQ)^{j_1}P^l$, kde $0\leq l<2$ a



Obrázok 9: Grupa $pg_1(a,b)$

b) $(P^2)^{k_2}(QP)^{j_1}Q^l$, kde $0 \leq l < 2$.

a)
Keďže prvok P^2 patrí do centra, potom doň patrí aj jeho inverz, čiže prvok P^{-2}. Teda

$$(P^2)^{k_2}(PQ)^{j_1}P^l = (P^2)^{k_2}(P^2)^{j_1}(P^{-2}PQ)^{j_1}P^l = (P^2)^{k_2+j_1}(P^{-1}Q)^{j_1}P^l.$$

Z prezentácie vieme, že rád prvku P^2 delí b a rád prvku $P^{-1}Q$ delí a. Potom podľa vety 5.4 existujú prirodzené čísla p, k, r, j také, aby platilo: $k_2+j_1 = pb+k$, kde $0 \leq k < b$ a $j_1 = ra+j$, kde $0 \leq j < a$. Môžme teda písať.

$$(P^2)^{k_2+j_1}(P^{-1}Q)^{j_1}P^l = (P^2)^{pb+k}(P^{-1}Q)^{ra+j}P^l = ((P^2)^b)^p(P^2)^k((P^{-1}Q)^a)^r(P^{-1}Q)^jP^l =$$

$$= 1^p(P^2)^k1^r(P^{-1}Q)^jP^l = (P^2)^k(P^{-1}Q)^jP^l, \text{ kde } 0 \leq k < b,\ 0 \leq j < a,\ 0 \leq l < 2.$$

Teda prvok je požadovaného tvaru.
b)
Začneme rovnako ako v bode a). Dostávame:

$$(P^2)^{k_2}(QP)^{j_1}Q^l = (P^2)^{k_2}(P^2)^{j_1}(P^{-2}QP)^{j_1}Q^l = (P^2)^{k_2+j_1}(Q^{-2}QP)^{j_1}Q^l = (P^2)^{k_2+j_1}(Q^{-1}P)^{j_1}Q^l.$$

Platí nasledujúca rovnosť $Q^{-1}P = (P^{-1}Q)^{-1}$. Keď to aplikujeme na náš tvar, dostávame:

$$\begin{aligned}(P^2)^{k_2+j_1}(Q^{-1}P)^{j_1}Q^l &= (P^2)^{k_2+j_1}(P^{-1}Q)^{-j_1}Q^l = (P^2)^{k_2+j_1}(P^{-1}Q)^{a-j_1}Q^l \\ &= (P^2)^{k_2+j_1}(P^{-1}Q)^{a-j_1-l}\ \underbrace{(P^{-1}Q)^l}_{l \text{ je 0 alebo 1}}\ Q^l = (P^2)^{k_2+j_1}(P^{-1}Q)^{a-j_1-l}\ \underbrace{P^{-l}Q^{2l}}_{=P^l} \\ &= (P^2)^{k_2+j_1}(P^{-1}Q)^{a-j_1-l}P^l.\end{aligned}$$

Ďalej postupujeme rovnako ako v bode a).
Z článku [*I.*] vieme, že veľkosť grupy $pg_1(a,b)$ je $2ab$ a keďže každý prvok sa dá napísať v jednom z $2ab$ tvarov, potom daný prvok je jednoznačne daný.
čbtd

Príklad 5.1 V nasledujúcich vetách sa budeme často odvolávať na výsledok násobenia dvoch ľubovoľných prvkov. V tomto príklade si ho odvodíme. Najprv si ale odvoďme, čomu sa rovná prvok $P^l(P^{-1}Q)^jP^{-l}$, kde $l \in \{0,1\}$. Nech $l = 0$, potom $P^0(P^{-1}Q)^jP^{-0} = (P^{-1}Q)^j = (P^{-1}Q)^{(-1)^0 j}$.

Nech $l = 1$, potom $P^1(P^{-1}Q)^jP^{-1} = (QP^{-1})^j = (PQ^{-1})^{-j} = (P^{-2}P\underbrace{P^2}_{Q^2}Q^{-1})^{-j} = (P^{-1}Q)^{(-1)^1 j}$.

Teda pre l patriace do množiny $\{0,1\}$ bude prvok $P^l(P^{-1}Q)^jP^{-l} = (P^{-1}Q)^{(-1)^l j}$. Teraz môžme prejsť ku všeobecnému tvaru súčinu dvoch ľubovoľných prvkov. Už pri dokazovaní kanonického tvaru prvku grupy $pg_1(a,b)$ sme využívali poznatok, že prvok P^2 patrí do centra.

$$\begin{aligned}(P^2)^k(P^{-1}Q)^jP^l(P^2)^{k'}(P^{-1}Q)^{j'}P^{l'} &= (P^2)^{k+k'}(P^{-1}Q)^jP^l(P^{-1}Q)^{j'}P^{-l}P^lP^{l'} = \\ &= (P^2)^{k+k'}(P^{-1}Q)^j(P^{-1}Q)^{(-1)^l j'}P^{l+l'} = (P^2)^{k+k'}(P^{-1}Q)^{j+(-1)^l j'}P^{l+l'}\end{aligned}$$

Odpoveď na otázku, kedy je predchádzajúca grupa izomorfná inej nám opäť podáva štruktúra jej centra.

Veta 5.8 *Centrum grupy $pg_1(a,b)$ danej prezentáciou (14) má veľkosť*

a) b, ak a je nepárne väčšie ako 1,

b) $2b$, ak a je párne väčšie ako 2

c) ak $a = 1$ potom centrom je celá cyklická grupa

d) ak $a = 2$ potom centrom je celá grupa izomorfná grupe $Z_{2b} \times Z_2$.

Dôkaz: Postupovať budeme priamo, ukážeme, aké prvky patria do centra. Aby nejaký prvok patril do centra musí platiť nasledujúca rovnosť:
$(P^2)^k(P^{-1}Q)^jP^l(P^2)^{k'}(P^{-1}Q)^{j'}P^{l'} = (P^2)^{k'}(P^{-1}Q)^{j'}P^{l'}(P^2)^k(P^{-1}Q)^jP^l$ pre pevne danú trojicu (k,j,l) a ľubovoľnú trojicu (k',j',l'). V predchádzajúcom príklade sme si odvodili, ako vyzerá výsledok násobenia ľubovoľných dvoch prvkov. Teda po využití tohto príkladu dostávame:

$$(P^2)^{k+k'}(P^{-1}Q)^{j+(-1)^l j'}P^{l+l'} = (P^2)^{k+k'}(P^{-1}Q)^{j'+(-1)^{l'} j}P^{l+l'}.$$

Vďaka tomu, že prvok je jednoznačne daný tvarom (15), potom zrejme platí:

$$\begin{aligned}k + k' &= k' + k \\ j + (-1)^l j' &= j' + (-1)^{l'} j \\ l + l' &= l' + l.\end{aligned}$$

Prvá a tretia rovnosť platia pre každé dve dvojice čísel (k,l), (k',l'). Veľkosť centra budú teda udávať dvojice (j,l), ktoré budú riešením druhej rovnice. Tá musí platiť pre každé l', teda aj pre $l' = 0$, ak to dosadíme do druhej rovnice, dostávame: $j + (-1)^l j' = j' + j$, odtiaľ $(-1)^l j' = j'$. Táto rovnosť musí platiť pre každé j', preto $l = 0$. Ak tento výsledok dosadíme do druhej rovnosti a za l' dosadíme 1, potom: $j + j' = j' - j$, odtiaľ $2j \equiv 0 \pmod a$. To znamená, ak a je nepárne a väčšie ako 1, potom do centra patria len mocniny prvku (P^2) a tých je b. Ak a je párne a väčšie ako 2, potom do centra patria také prvky $(P^2)^k(P^{-1}Q)^j$, kde k je ľubovoľné a j je 0 alebo $\frac{a}{2}$. Týmto sú dokázané časti a) a b).

Nech $a = 1$, potom z prezentácie: $P^{-1}Q = 1$ a teda $P = Q$, čo znamená, že grupa je cyklická veľkosti $2b$.

Nech $a = 2$, potom $P^{-1}Q$ je involúcia a platí: $(P^{-1}Q)^{-1} = P^{-1}Q$, odkiaľ $Q^{-1}P = P^{-1}Q$. Prenásobme obe strany rovnosti zľava prvkom $P^2(= Q^2)$. Dostávame: $QP = PQ$, čo znamená, že generátory navzájom komutujú a teda grupa je abelovská. Ešte nám ostáva dokázať izomorfizmus medzi grupou $pg_1(2,b)$ a grupou $Z_{2b} \times Z_2$. V kapitole o štrukturálnych vlastnostiach grupy $p1(a,b;c)$ sme uviedli vetu 4.1, ktorá hovorí o izomorfizmoch abelovských grúp.

Musíme určiť exponent, tým je ale číslo $lcm(Order(P), Order(Q))$. Keďže vieme, že $P^2 = Q^2$, potom majú oba prvky (P a Q) rovnaký rád. Nech to neplatí, bez ujmy na všeobecnosti môžeme predpokladať, že rád prvku Q je menší ako rád prvku P (ak by platila opačná nerovnosť, potom by v nasledujúcich riadkoch bol prvok Q preznačený za P a naopak). Nech je párny. Potom $P^{Order(Q)} =$

$Q^{Order(Q)} = 1$, čo znamená, že rád prvku P delí rád prvku Q. Čo je v spore s predpokladom, že rád prvku Q je menší ako rád prvku P. Nech je teraz rád prvku Q nepárny, potom $P^{Order(Q)+1} = Q^{Order(Q)+1} = Q$, čo znamená, že grupa je cyklická, generovaná prvkom P, čo je však v spore s veľkosťou grupy. Teda platí $Order(P) = Order(Q)$. To ale znamená, že exponentom je číslo $Order(P)$ a keďže je grupa generovaná dvoma prvkami, potom je izomorfná grupe: $Z_{Order(P)} \times Z_{\frac{4b}{Order(P)}} = Z_{2b} \times Z_2$.
čbtd

Na dôkaz vety o izomorfizmoch potrebujeme ešte poznať počet involúcií.

Veta 5.9 *Grupa $pg_1(a,b)$ má*

a) 1 involúciu, ak a je nepárne a b párne,

b) 3 involúcie, ak a, b sú párne,

c) a involúcií, ak a, b sú nepárne a

d) $a+1$ involúcií, ak a je párne a b nepárne.

Dôkaz: Znovu sa budeme odvolávať na príklad 1. Ak je prvok involúciou, musí platiť:
$(P^2)^k(P^{-1}Q)^jP^l(P^2)^k(P^{-1}Q)^jP^l = (P^2)^{2k}(P^{-1}Q)^{j+(-1)^lj}P^{2l} = (P^2)^{2k+l}(P^{-1}Q)^{j+(-1)^lj} = 1$.
Vzhľadom na to, že prvok je jednoznačne daný tvarom (15), potom musí platiť:

$$2k + l = b \text{ alebo } 2k + l = 0$$
$$j + (-1)^l j = a \text{ alebo } j + (-1)^l j = 0.$$

Nech $l = 0$. Potom z prvých dvoch rovníc dostávame: $k = \frac{b}{2}$ alebo $k = 0$. Z ďalších dvoch rovníc dostávame: $j = \frac{a}{2}$ alebo $j = 0$.

Nech $l = 1$. Z prvých dvoch rovníc dostávame: $k = \frac{b-1}{2}$ alebo $k = -\frac{1}{2}$. Keďže k môže byť len prirodzené číslo, potom pre $l = 1$ pripadá do úvahy len prvá časť riešenia. Z prvej rovnice druhého riadku ale pre $l = 1$ riešenie neexistuje, pre druhú rovnicu je riešením každé $j \in \{0, 1, ..., a-1\}$

Ak to zhrnieme, potom:

a) Nech a je nepárne a b párne. Potom pre $l = 1$ nedostávame žiadne riešenie pre k a teda l musí byť nulové. Potom $k = \frac{b}{2}$ alebo $k = 0$. Keďže a je nepárne, potom $j = 0$. Riešením pre prvý prípad sú teda dve trojice čísel (k, j, l) a to: $(\frac{b}{2}, 0, 0)$ a $(0, 0, 0)$. Druhá trojica ale určuje jednotkový prvok, čo involúciou nie je. Tým je dokázaná táto časť vety.

b) Nech a aj b sú párne. Potom rovnako ako v bode a) $l = 0$. Teda $k = \frac{b}{2}$ alebo $k = 0$. a je teraz párne, teda $j = 0$ alebo $j = \frac{a}{2}$. Pre k aj pre j existujú dve riešenia a preto sú dokopy 4 riešenia, medzi ktorými je ale znovu triviálny prvok.

c) Nech a aj b sú nepárne. Pre $l = 0$ dostávame jedinú trojicu riešenia, a to $(0, 0, 0)$, čo ale involúciou nie je, preto $l = 1$. Potom $k = \frac{b-1}{2}$ a j je ľubovoľné. Teda, pre výber k a l máme len po jednej možnosti výberu, pre výber j ich je dokopy a. Celkovo je v tomto prípade a involúcií.

d) Nech a je párne a b nepárne. Pre $l = 0$ dostávame dve trojice riešenia a to $(0, 0, 0)$ a $(0, \frac{a}{2}, 0)$. Prvé riešenie je znovu jednotkový prvok, teda pre $l = 0$ existuje jediná inovolúcia. Pre $l = 1$ postupujeme rovnako ako v bode c), kde sme dostali dokopy a involúcií. V tomto prípade je teda $a + 1$ rôznych involúcií.

čbtd

Teraz môžme konečne vysloviť vetu o izomorfizme grupy $pg_1(a,b)$ s grupou $pg_1(a',b')$.

Veta 5.10 *Grupy $pg_1(a,b)$ a $pg_1(a',b')$ sú izomorfné, vtedy a len vtedy ak $(a,b) = (a',b')$.*

Dôkaz:
(„⇐")
Nech $(a,b) = (a',b')$, potom sa jedná o rovnakú grupu, teda grupy $pg_1(a,b)$ a $pg_1(a',b')$ sú izomorfné.
(„⇒")
Nech $pg_1(a,b)$ je s $pg_1(a',b')$ izomorfná, potom máme dokázať, že $(a,b) = (a',b')$. Dokážeme to sporom, nech teda $(a,b) \neq (a',b')$ a predpokladajme, že dané grupy izomorfné sú.

I. Nech je a párne a väčšie ako 2. Potom centrum prvej grupy má veľkosť $2b$.

   a) Nech je teda a' párne a väčšie ako 2. Veľkosť centra druhej grupy bude $2b'$. Z toho vyplýva, že $2b = 2b'$ teda $b = b'$ a $2ab = 2a'b'$, využitím predchádzajúceho výsledku $ab = a'b$ a teda $a = a'$. Čo je spor s predpokladom, že $(a,b) \neq (a',b')$

   b) Nech je a' nepárne a väčšie ako 1. Veľkosť centra $pg_1(a',b')$ je b'. Opäť využitím rovnosti veľkostí grúp dostávame: $b' = 2b$ a teda $a' = \frac{a}{2}$. Prvá grupa má ale minimálne 3 involúcie. V druhej je a' nepárne a b' párne, čo využitím predchádzajúcej vety znamená, že má len 1 involúciu. To je však v spore s izomorfizmom.

   c) Nech je $a' = 1$ alebo $a' = 2$. Potom veľkosť centra druhej grupy je $2a'b$, teda celá grupa je abelovská, čo grupa $pg_1(a,b)$ nie je.

II. Nech je a nepárne a väčšie ako 1. Centrum prvej grupy má veľkosť b.

   d) Nech a' je párne a väčšie ako 2. Hľadajme teraz izomorfizmus z druhej grupy $pg_1(a',b')$ do prvej grupy $pg_1(a,b)$. To, že $(a,b) = (a',b')$ sme už dokázali v bode $I.b$).

   e) Nech a' je nepárne a väčšie ako 1. Aj veľkosť centra druhej grupy(čo sa rovná b') musí byť b. Teda platí $b = b'$ a využitím rovnosti veľkostí grúp: $a = a'$. To je však v spore s predpokladmi.

   f) Nech $a' = 1$ alebo $a' = 2$. Potom neizomorfnosť sa dokáže analogicky ako v bode $I.c$).

III. Nech je $a = 1$ alebo $a = 2$. Potom je celá grupa $pg_1(a,b)$ abelovská.

   g) Nech $a' > 2$, potom ale grupa $pg_q(a',b')$ abelovská nie je, teda grupy $pg_1(a,b)$ a $pg_1(a',b')$ izomorfné nie sú.

   h) Nech $a' = 1$. Potom je grupa cyklická s rádom $2b$. Ak $a = 2$, potom grupa $pg_1(2,b)$ cyklická nie je, a teda grupy izomorfné nie sú. Ak $a = 1$ potom je grupa $pg_1(1,b)$ cyklická s rádom $2b'$. Aby boli izomorfné, musí platiť: $2b = 2b'$ a teda $(1,b) = (1,b')$, čo je v spore s predpokladom nerovnosti parametrov.

   i) Nech $a' = 2$. Táto grupa je izomorfná grupe $Z_{2b'} \times Z_2$, teda cyklická nie je a potom nie je izomorfná grupe $pg_1(1,b)$. Ak $a = 2$, potom je grupa $pg_1(2,b)$ izomorfná $Z_{2b} \times Z_2$. Z veľkosti grúp ale vyplýva, že $2b = 2b'$ a teda parametre sa rovnajú.

Iné prípady už nastať nemôžu, veta je týmto dokázaná.
čbtd

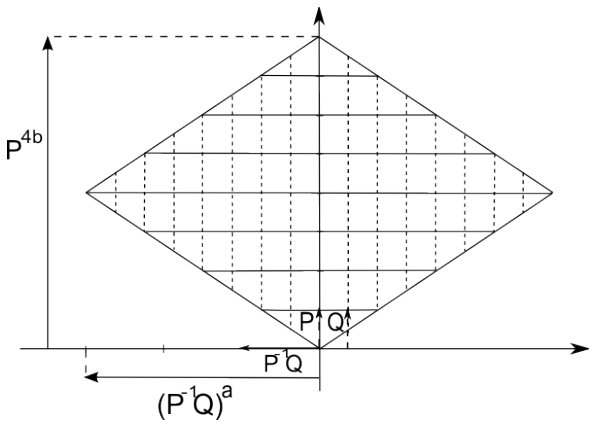
5.4 Štrukturálne vlastnosti grupy $pg_2(a,b)$

Ďalšou tapetovou grupou je $pg_2(a,b)$. Vďaka svojej štruktúre, ktorá je veľmi podobná štruktúre grupy $pg_1(a,b)$ bude omnoho ľahšie dokazovať niektoré jej vlastnosti. Jej prezentácia je daná nasledovným predpisom:

$$pg_2(a,b) := \left\langle P, Q | P^2Q^{-2} = (P^{-1}Q)^a P^{2b} = P^{4b} = 1 \right\rangle. \tag{16}$$

Nasledujúci obrázok nám udáva, ako vyzerá grupa $pg_2(a,b)$ v geometrickej interpretácii.

Nielen prezentáciou sa táto grupa ponáša na svoju predchodkyňu, ale aj svojimi vlastnosťami. Hneď štruktúra každého jej prvku to dokazuje.



Obrázok 10: Grupa $pg_2(a,b)$

Veta 5.11 *Každý prvok grupy $pg_2(a,b)$ je tvaru:*

$$(P^2)^k(P^{-1}Q)^jP^l, \text{ kde } k\in\{0,1,...,2b-1\}\,,\ j\in\{0,1,...,a-1\}\ \text{ a } l\in\{0,1\}\,. \tag{17}$$

Dôkaz: Dôkaz tejto vety bude úplne analogický dôkazu o štruktúre prvku grupy $pg_1(a,b)$. Nastáva tu jediný rozdiel (okrem rádov prvkov) a to, že $(P^{-1}Q)^a = P^{2b}$. Teda, keď už dospejeme do tvaru $(P^2)^{k'}(P^{-1}Q)^{j'}P^l$, kde $0\le k'<2b,\ 0\le j'<2a,\ 0\le l<2$, využijeme znovu vetu 5.4, čo znamená, existujú také prirodzené čísla p,q,k,j, pre ktoré platí: $j'=pa+j$, kde $0\le j<a$ a $k'+pb=2bq+k$, kde $0\le k<2b$. Po konečnej úprave:

$$(P^2)^{k'}(P^{-1}Q)^{j'}P^l=(P^2)^{k'}(P^{-1}Q)^{pa+j}P^l=(P^2)^{k'}((P^{-1}Q)^a)^p(P^{-1}Q)^jP^l=$$

$$=(P^2)^{k'}((P^2)^b)^p(P^{-1}Q)^jP^l=(P^2)^{k'+pb}(P^{-1}Q)^jP^l=(P^2)^{2bq+k}(P^{-1}Q)^jP^l=$$

$$=(P^{4b})^q(P^2)^k(P^{-1}Q)^jP^l=1^q(P^2)^k(P^{-1}Q)^jP^l=(P^2)^k(P^{-1}Q)^jP^l.$$

Kde $0\le k<2b,\ 0\le j<a,\ 0\le l<2$. Teda každý prvok je tvaru (17).
čbtd

Aby sme mohli vysloviť vetu o izomorfizomch, potrebujeme ešte poznať veľkosť centra.

Veta 5.12 *Centrum grupy $pg_2(a,b)$ má veľkosť $2b$, keď $a\ge 2$ alebo centrom grupy $pg_2(a,b)$ je celá grupa, ak $a=1$.*

Dôkaz: Nech $a\neq 1$. Postupujme rovnako ako v prípade grupy $pg_1(a,b)$, to je vyjadrime si súčin ľubovoľných dvoch prvkov grupy $pg_2(a,b)$ podobne ako v príklade 5.1(keďže relácie v grupách sú podobné, budú aj súčiny podobné). Dostávame rovnosti:

$$k+k'=k'+k$$
$$j+(-1)^lj'=j'+(-1)^{l'}j$$
$$l+l'=l'+l$$

Prvá a posledná z rovností platia pre každé l, l' a k,k'.
Keďže druhá rovnosť musí nastať pre každé l', tak aj pre $l'=0$. Po dosadení dostaneme:

$$(-1)^lj'-j'=0.$$

Táto rovnosť musí byť ale splnená pre každé j', teda aby sa prvok nachádzal v centre, musí platiť $l=0$. Ale rovnosť musí nastať aj v prípade, že $l'=1$. Po dosadení:

$$2j\equiv 0 \pmod{2a}.$$

Čo znamená, že buď $j = 0$, alebo $j = a$, čo by ale znamenalo, že do centra patrí každý prvok tvaru: $(P^2)^k(P^{-1}Q)^a$ pre každú voľbu k. Ale z prezentácie vieme, že $(P^{-1}Q)^a = P^{2b}$, teda ak dosadíme: $(P^2)^k(P^2)^b = (P^2)^{k+b}$, pre každé $k \in \{0, 1, ..., 2b-1\}$. Čo ale znamená, že aj číslo $k + b$ bude do spomínanej množiny patriť. Teda, do centra patria len mocniny P^2.

Nech $a = 1$. Potom, postupujeme rovnako ako pri centre grupy $pg_1(2, b)$, keďže aj v tomto prípade je prvok $P^{-1}Q$ rádu 2. Dostaneme, že generátory grupy navzájom komutujú a teda je celá grupa abelovská.
čbtd

To, že dve grupy pg_2 s rôznymi parametrami nie sú nikdy izomorfné, je priamy dôsledok predchádzajúcej vety.

Dôsledok 5.2 *Ak $(a, b) \neq (a', b')$, potom grupy $pg_2(a, b)$ a $pg_2(a', b')$ nie sú izomorfné.*

Dôkaz: Keďže veľkosť grupy je $4ab$ a veľkosť centra každej grupy $pg_2(a, b)$ je $2b$, potom keďže predpokladáme, že naše grupy sú izomorfné platí: $2b = 2b'$, čize $b = b'$ a odtiaľ aj $a = a'$.

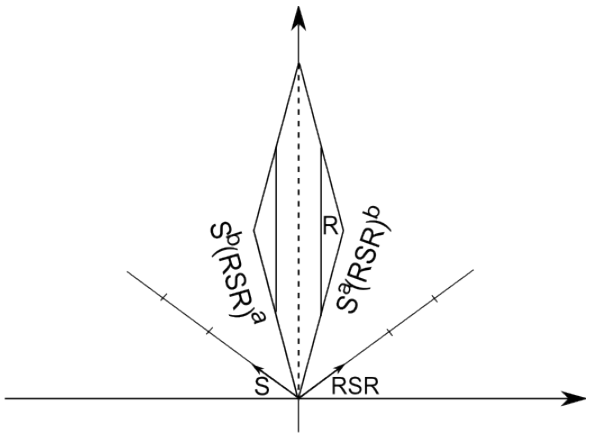
Nech je grupa $pg_2(a, b)$ abelovská, potom musí byť aj grupa $pg_2(a', b')$ abelovská. Ale abelovské sú jedine v prípade, že $a = a' = 1$, potom z rovnosti rádov grúp $b = b'$.
čbtd

5.5 Štrukturálne vlastnosti grupy $cm_1(a, b)$

Grupu $cm_1(a, b)$ generujú reflexia a posunutie, ktoré nie je s osou reflexie rovnobežné, jej geometrickú prezentáciu si môžeme prezrieť na obrázku (11). Jej prezentácia je daná nasledovným predpisom:

$$cm_1(a, b) := \langle R, S | (RS)^2 = (SR)^2; R^2 = S^a(RSR)^b = S^b(RSR)^a = 1 \rangle . \tag{18}$$

Nájdeme si všeobecný tvar prvku.



Obrázok 11: Grupa $cm_1(a, b)$

Veta 5.13 *Každý prvok grupy $cm_1(a, b)$ danej prezentáciou (18) je určený tvarom:*

$$S^k(RSR)^j R^i, \tag{19}$$

kde $i \in \{0, 1\}$, $j \in \{0, 1, ..., gcd(a, b) - 1\}$ a k je ľubovoľné celé číslo.

Dôkaz: Každá postupnosť tvaru $S^{p_1}R^{q_1}S^{p_2}...$ určuje v grupe $cm_1(a, b)$ nejaký prvok. Keďže z prezentácie (18) vyplýva, že R je involúcia, potom sa nám stačí zamerať na postupnosti tvaru: $S^{p_1}RS^{p_2}R...(1)$. Z prezentácie ďalej vieme, že $(RS)^2 = (SR)^2$, čo môžeme prepísať do tvaru $RSRS =$

$SRSR$. V grupe platí asociatívny zákon a teda: $(RSR)S = S(RSR)$, čo znamená, že prvky S a RSR spolu komutujú. Ďalej z toho, že R je involúcia vyplýva: $RS^kR = \underbrace{RSRRSRRSR...RSR}_{k \text{ - krát}} = (RSR)^k$.

Upravme postupnosť (1).

$$S^{p_1}(RSR)^{p_2}S^{p_3}(RSR)^{p_4}... = S^{p_1+p_3+\cdots}(RSR)^{p_2+p_4+\cdots}R^i = S^{k_1}(RSR)^{j_1}R^i.$$

Z prezentácie ďalej vieme, že $S^a(RSR)^b = S^b(RSR)^a = 1$. Z tejto rovnosti vyplýva, že do podgrupy $H = \langle S\rangle \cap \langle RSR\rangle$ patria prvky $(RSR)^a$ a tiež $(RSR)^b$. Nech $gcd(a,b) = ma + nb$. Keďže je H podgrupou, patrí do nej aj súčin ľubovoľných mocnín hocijakých prvkov do nej patriacich. Teda prvok $(RSR)^{gcd(a,b)} = (RSR)^{ma+nb} = ((RSR)^a)^m((RSR)^b)^n \in H$. Z toho nám vyplýva, že $(RSR)^{j_1} = (RSR)^{lgcd(a,b)+q} = S^{lr}(RSR)^q$, kde $(RSR)^{gcd(a,b)} = S^r$ a $0 \leq q < gcd(a,b)$. Týmto sme dokázali vetu.

čbtd

Tu prichádza otázka, aké je číslo r v predchádzajúcom dôkaze. Vieme, že $(RSR)^a = S^{-b}$ a $(RSR)^b = S^{-a}$ a teda $S^r = (RSR)^{gcd(a,b)} = (RSR)^{ma}(RSR)^{nb} = S^{-mb-na}$, čo znamená, že $r = -(mb+na)$.

Aby sme ohraničili množinu, do ktorej bude patriť k, budeme potrebovať vedieť rád prvku S.

Veta 5.14 *Rád prvku S v grupe $cm_1(a,b)$ je $\frac{|a^2-b^2|}{gcd(a,b)}$.*

Dôkaz: Budeme vychádzať zo vzťahu: $Order(H.G) = \frac{Order(H\times G)}{Order(H\cap G)}(\bullet)$, kde H, G sú ľubovoľné dve grupy, množina $H.G = \{hg; h \in H; g \in G\}$ a $H \times G$ je kartézsky súčin. Nech grupa $H := \langle S\rangle$ a grupa $G := \langle RSR\rangle$. Keďže RSR je konjugáciou prvku S prvkom R a konjugácie zachovávajú rády, potom $Order(H \times G) = Order(H).Order(G) = Order(S).Order(RSR) = Order(S)^2$. Ďalej z toho, že prvky S a RSR navzájom komutujú, vyplýva $H.G = \langle S, RSR\rangle$. Táto podgrupa grupy $cm_1(a,b)$ je indexu 2 a keďže z článku [*I.*] vieme, že veľkosť grupy $cm_1(a,b)$ je $2|a^2 - b^2|$, potom $Order(H.G) = |a^2 - b^2|$.

V dôkaze predchádzajúcej vety sme si ukázali, že $\left\langle (RSR)^{gcd(a,b)}\right\rangle$ je podgrupou grupy $H \cap G$. Nech $(RSR)^k \in H \cap G$ a zároveň $(RSR)^k \neq (RSR)^{l.gcd(a,b)}$. Potom existuje nejaký exponent n, pre ktorý bude platiť $(RSR)^k = S^n$, potom $S^{-n}(RSR)^k = 1 = S^a(RSR)^b = S^b(RSR)^a$. Teda, existujú také celé čísla p a q, pre ktoré bude platiť $(-n,k) = p(a,b) + q.(b,a)$. Keďže hľadáme k, musíme vyriešiť rovnicu $k = pb + qa$. Takáto rovnica má podľa vety 4.4 riešenie v celých číslach jedine v prípade, že $gcd(a,b)|k$, tým sme dokázali, že okrem prvkov patriacich do $\left\langle (RSR)^{gcd(a,b)}\right\rangle$ už žiaden iný prvok do podgrupy $H \cap G$ nepatrí. Veľkosťou tejto grupy je ale $\frac{Order(S)}{gcd(gcd(a,b),Order(S))}$.

Vráť me sa k vzťahu $(\bullet)$.

$$|a^2 - b^2| = \frac{Order(S)^2}{\frac{Order(s)}{gcd(gcd(a,b),Order(S))}} = Order(S).gcd(gcd(a,b), Order(S))$$

$$Order(S) = \frac{|a^2 - b^2|}{gcd(gcd(a,b), Order(S))} = \frac{(gcd(a,b))^2|a'^2 - b'^2|}{gcd(gcd(a,b), Order(S))}$$

Kde $a' = \frac{a}{gcd(a,b)}$ a $b' = \frac{b}{gcd(a,b)}$. Vzhľadom na to, že $gcd(gcd(a,b), Order(S)) \leq gcd(a,b)$, potom z pravej strany rovnosti vyplýva $gcd(a,b)|Order(S)$.

$$Order(S) = \frac{|a^2 - b^2|}{gcd(a,b)}.$$

čbtd

Vetami 5.13 a 5.14 sme dokázali, že každý prvok patriaci do grupy $cm_1(a,b)$ je tvaru (19), kde $k \in \left\{0, 1, ..., \frac{|a^2-b^2|}{gcd(a,b)} - 1\right\}$, $j \in \{0, 1, ..., gcd(a,b) - 1\}$ a $i \in \{0, 1\}$, čo je dokopy $2|a^2 - b^2|$ tvarov. Taký istý je rád grupy $cm_1(a,b)$, čo znamená, že prvok tvaru (19) je určený jednoznačne.

Na určenie parametrov, kedy sú grupy $cm_1(a,b)$ a $cm_1(a',b')$ izomorfné, nám postačí vedieť, aké veľké je centrum grúp.

Veta 5.15 *Veľkosť centra grupy $cm_1(a,b)$ je $a+b$, ak $|a-b| \neq 1$ alebo centrom je celá grupa $cm_1(a,b)$, ak $|a-b| = 1$.*

Dôkaz: Nech $|a-b| \neq 1$.

Aby prvok patril do centra, musí komutovať s každým prvkom grupy. Stačí ale zistiť, ktoré prvky komutujú s oboma generátormi, teda pre aké k, j, i platí $RS^k(RSR)^jR^iR = S^k(RSR)^jR^i = SS^k(RSR)^jR^iS^{-1}$.

$$SS^k(RSR)^jR^iS^{-1} = S^{k+i}(RSR)^{j-i}R^i$$

V tomto bode sme využili, že v prípade nulového i prvok S^{-1} komutuje s RSR, v prípade, že $i = 1$, bude $RS^{-1} = (RSR)^{-1}R$.

Prvok na pravej strane rovnosti sa rovná prvku $S^k(RSR)^jR^i$ práve vtedy, ak $i = 0$. To vyplýva z jednoznačnosti tvaru každého prvku. Teraz ukážeme, ktoré prvky komutujú s R.

$$RS^k(RSR)^jR^iR = (RSR)^kS^jRR^iR = S^j(RSR)^kR^i$$

Využívali sme, že asociatívny zákon v grupách a $(RSR)^j = RS^jR$. Znovu, ak sa má prvok $S^j(RSR)^kR^i$ rovnať prvku $S^k(RSR)^jR^i$, musí platiť $j = k$.

Ak má prvok patriť do centra, musí platiť $i = 0$ a $j = k$. Teda, prvok musí byť tvaru $S^k(RSR)^k$, kde k je ľubovoľné. Keďže z prezentácie (18) vieme, že $RSRS = SRSR$, potom S^k komutuje s $(RSR)^k$ pre každé k. Potom centrom je cyklická grupa generovaná prvkom $S(RSR)$. Nech $Order(S(RSR)) = r$, nech $r = n.gcd(a,b) + m$, kde $0 \leq m < gcd(a,b)$ a nech $gcd(a,b) = pa + qb$, potom
$(S(RSR))^r = S^r(RSR)^r = S^r(RSR)^{n.gcd(a,b)+m} = S^r((RSR)^{gcd(a,b)})^n(RSR)^m =$
$= S^{r-n(pb+qa)}(RSR)^m = 1$. Z čoho vyplýva, že $m = 0$ a teda $r = n.gcd(a,b)$.

$$(S(RSR))^{n.gcd(a,b)} = S^{n(pa+qb)-n(pb+qa)} = S^{n(a-b)(p-q)} = 1$$

Stačí nám hľadať rád prvku $S^{(a-b)(p-q)}$, to je ale číslo

$$\begin{aligned}\frac{Order(S)}{gcd((a-b)(p-q), Order(S))} &= \frac{\frac{|(a-b)(a+b)|}{gcd(a,b)}}{gcd(|(a-b)(p-q)|, \frac{|(a-b)(a+b)|}{gcd(a,b)})} \\ &= \frac{|a-b|.\frac{a+b}{gcd(a,b)}}{(a-b).gcd(p-q, \frac{a+b}{gcd(a,b)})} \\ &= \frac{\frac{a+b}{gcd(a,b)}}{gcd(p-q, a'+b')}\end{aligned}$$

Využili sme, že $gcd(a,b)|(a+b)$ a tiež, že v operácii gcd platí distributívny zákon a použili označenie $a' = \frac{a}{gcd(a,b)}$ a $b' = \frac{b}{gcd(a,b)}$. Teraz ukážeme, že $gcd(p-q, a'+b') = 1$. Keďže sme si vybrali p a q také, aby platilo $pa+qb = gcd(a,b)$, bude platiť $pa'+qb' = p(a'+b') - pb' + qb' = p(a'+b') - b'(p-q) = 1$. Toto je diofantická rovnica, ktorá má riešenie podľa vety 4.4 práve vtedy, keď $gcd(a'+b', p-q)|1$, z čoho automaticky $gcd(p-q, a'+b') = 1$.

Potom $Order(S^{(a-b)(p-q)}) = \frac{a+b}{gcd(a,b)}$ a $Order(S(RSR)) = gcd(a,b).\frac{a+b}{gcd(a,b)} = a+b$.

Nech $|a-b| = 1$.

Z prezentácie (18) vieme, že $S^a(RSR)^b = S^b(RSR)^a$, teda $S^{a-b} = (RSR)^{a-b} = RS^{a-b}R$, z čoho vidíme, že R a $S^{|a-b|} = S$ spolu komutujú. Keďže $gcd(a,b) = gcd(max(a,b), max(a,b)-1) = 1$, bude každý prvok grupy $cm_1(a,b)$ vyzerať S^kR^i. Ukázali sme si, že S a R spolu komutujú a teda, celá grupa $cm_1(a,b)$ je abelovská.

čbtd

Vďaka tomu, že poznáme veľkosti centier jednotlivých grúp $cm_1(a,b)$, môžeme dokázať vetu o izomorfizmoch.

Veta 5.16 *Grupy $cm_1(a,b)$ a $cm_1(a',b')$ sú izomorfné práve vtedy, keď $(a,b) = (a',b')$ alebo $(a,b) = (b',a')$.*

Dôkaz: Ak $(a,b) = (a',b')$, potom sa jedná o jednu grupu a izomorfizmom bude každý automorfizmus. Nech $(a,b) = (b,a)$. Z prezentácie (18) ale vidieť, že sa bude jednať o rovnakú grupu, keďže sa len prehodia poradia rovností. A teda, izomorfizmom bude opäť hocijaký automorfizmus.

Nech sú grupy izomorfné. Potom bude platiť rovnosť rádov grúp aj rovnosť rádov centier grúp. Ak $|a-b| \neq 1$, potom grupa $cm_1(a,b)$ nie je abelovská a nemôže byť komutatívna ani $cm_1(a',b')$, preto platí $|a'-b'| \neq 1$. Ak berieme a a b ako konštanty a a' a b' ako neznáme, dostaneme sústavu dvoch rovníc o dvoch neznámych.

$$a+b = a'+b'$$
$$2|(a+b)(a-b)| = 2|(a'+b')(a'-b')|.$$

Vzhľadom na to, že platí prvá rovnosť, môžeme krátiť, dostaneme rovnice tvaru $a+b = a'+b'$ a $|a-b| = |a'-b'|$. Po vyriešení dostávame $a' = a$ alebo $a' = b$.

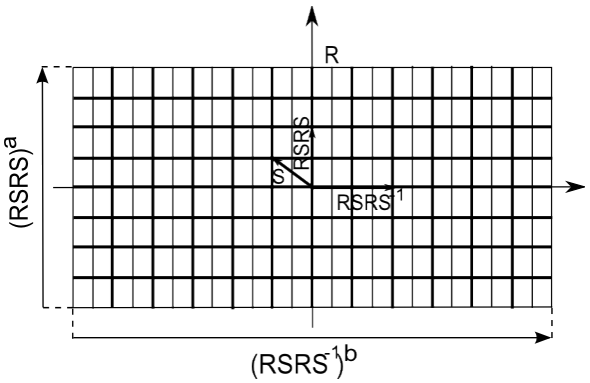
Ak $|a-b| = 1$, potom $cm_1(a,b)$ je komutatívna a preto musí platiť $|a'-b'| = 1$. Dostávame ale rovnaké rovnosti ako v predchádzajúcom prípade.
čbtd

5.6 Štrukturálne vlastnosti grupy $cm_2(a,b)$

Grupa $cm_2(a,b)$ podobne ako grupa $cm_1(a,b)$ je generovaná jednou reflexiou a jednou transláciou, ktorá nie je rovnobežná s osou reflexie. Jej prezentáciu určuje nasledujúci predpis:

$$cm_2(a,b) := \left\langle R,S | (RS)^2 = (SR)^2; R^2 = (RSRS)^a = (RSRS^{-1})^b = 1 \right\rangle. \tag{20}$$

Predstaviť si ju môžeme vďaka obrázku (12).



Obrázok 12: Grupa $cm_2(a,b)$

V tejto grupe nám stačí poznať veľkosť centra, aby sme povedali, kedy sú dve grupy izomorfné. Predtým si ale ukážeme, ako vyzerá každý prvok grupy $cm_2(a,b)$.

Veta 5.17 *Každý prvok grupy $cm_2(a,b)$ danej prezentáciou (20) má kanonický tvar:*

$$S^k(RSR)^j R^i, \tag{21}$$

kde $0 \leq k < \frac{2ab}{gcd(a,b)}, 0 \leq j < gcd(a,b)$ a $0 \leq i < 2$.

Dôkaz: To, že každý prvok grupy $cm_2(a,b)$ môžeme previesť do tvaru (21), kde k nie je ohraničené, by sme dokázali analogicky ako vo vete 6.12, kde $(RSR)^{gcd(a,b)} = (RSR)^{pa}(RSR)^{qb} = S^{-pa}S^{qb}$ a $gcd(a,b) = pa+qb$. Ohraničenie pre k a teda rád prvku S by sme odvodili podobne ako vo vete 6.13.
čbtd

Teraz už môžeme odvodiť veľkosť centra.

Veta 5.18 *Veľkosť centra grupy $cm_2(a,b)$ je $2a$, ak $b \neq 1$ a centrom je celá grupa, ak $b = 1$.*

Dôkaz: Veľkosť centra ukážeme podobne ako vo vete 6.14. V prípade, že $b \neq 1$, dostávame znovu, že ak má prvok $S^k(RSR)^jR^i$ patriť do centra, musí platiť $S^k(RSR)^jR^i = S^{k+i}(RSR)^{j-i}R^i = S^j(RSR)^kR^i$. Znovu prvok patrí do centra len pre nulové i. Po úprave $RS^{k-j}R = S^{k-j}$. Pre $k = j$ platí táto rovnosť triviálne, a podobne ako v prípade grupy $cm_1(a,b)$ bude prvok $SRSR$ súčasťou centra. Z prezentácie (20) vieme, že $(RSRS^{-1})^b = 1$ a tiež $RSRS = SRSR$, teda $(RSR)^b = S^b$, potom prvok S^b komutuje s R a patrí do centra. Keďže je centrum podgrupou, budú tam patriť aj všetky mocniny prvku S^b. Teda, prvok S^{k-j} patrí do centra práve vtedy, keď $k - j = l.b$. Pre číslo j máme $gcd(a,b)$ možností. Rád prvku S^b je $\frac{2a}{gcd(a,b)}$ a toľko je možností pre výber čísla l, keďže $l.b \leq Order(\langle S \rangle) = \frac{2ab}{gcd(a,b)}$, k je potom jednoznačne dané. Dokopy môžeme vybrať do centra $2a$ prvkov.

Nech do centra patrí aj iný prvok S^{lb+s}, kde l a s sú prirodzené čísla. Teda $RS^{lb+s}R = S^{lb+s}$, potom $S^{lb+s}(RSR)^{-lb-s} = S^a(RSR)^a = S^b(RSR)^{-b} = 1$, potom musí platiť rovnosť $(lb + s, -lb - s) = m(a,a) + n(b,-b)$, čo je sústava dvoch rovníc o dvoch neznámych. Po vyriešení $2ma = 0$, teda $m = 0$. Po dosadení dostávame rovnicu $lb + s = nb$, odtiaľ už vyplýva, že $b|s$.

Ak $b = 1$, potom $gcd(a,b) = 1$ a z prezentácie vieme, že do centra patrí prvok S. Ten potom komutuje aj s prvkom R, čiže centrom je celá grupa.
čbtd

Asi už teraz nebude prekvapením, kedy sú dve grupy $cm_2(a,b)$ a $cm_2(a',b')$ izomorfné.

Veta 5.19 *Grupy $cm_2(a,b)$ a $cm_2(a',b')$ sú izomorfné vtedy a len vtedy, ak $(a,b) = (a',b')$.*

Dôkaz: Zprava doľava je to triviálne vzhľadom na to, že sa jedná o rovnakú grupu.

Ak sú grupy $cm_2(a,b)$ a $cm_2(a',b')$ izomorfné, potom musia mať centrum rovnakej veľkosti, musí teda platiť: $2a = 2a'$ a odtiaľ a z následného využitia rovnosti rádov grúp plynie, že $(a,b) = (a',b')$. Ak $b = 1$, potom prvá z grúp je abelovská, potom musí byť abelovská aj druhá, teda $b' = 1$ a odtiaľ už $a = a'$.
čbtd

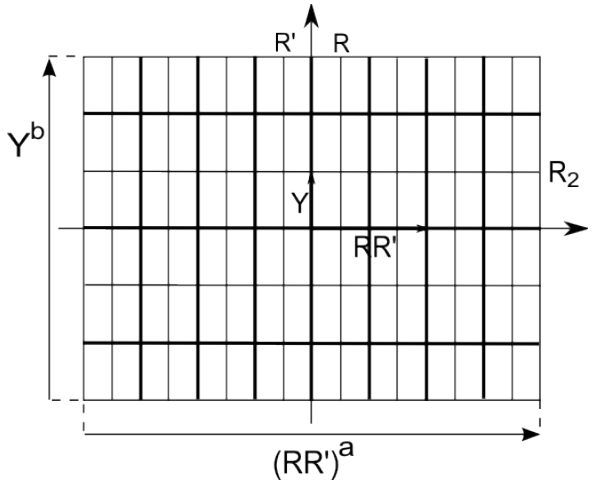
6 Grupy *pmm*, *pmg*, *pgg*

6.1 Štrukturálne vlastnosti grupy $pmm_1(a,b)$

Grupa $pmm_1(a,b)$ je určená troma reflexiami a jedným posunutím. Prezentácia je nasledovná:

$$pmm_1(a,b) := \langle R, R', R_2, Y | [R,Y] = [R',Y] = [R_2,R] = [R_2R'] = R^2 = \\ = R'^2 = R_2^2 = (RR')^a = Y^b = (R_2Y)^2 = 1 \rangle. \tag{22}$$

Predstavu o tom, ako táto grupa vyzerá v rovine nám dáva obrázok (13).



Obrázok 13: Grupa $pmm_1(a,b)$

Vďaka nasledujúcej vete budeme okamžite vedieť povedať, koľko má daná grupa involúcií a aké je jej centrum, stačí poznať niektoré vlastnosti dihedrálnych grúp.

Veta 6.1 *Grupa $pmm_1(a,b)$ daná prezentáciou (22) je izomorfná grupe:*

$$D_{2a} \times D_{2b}.$$

Dôkaz: Budeme dokazovať podobným spôsobom, ako v prípade grupy $pm_1(a,b)$. Dokážeme, že sa v grupe $pmm_1(a,b)$ normálne podgrupy D_{2a} a D_{2b}, ktoré majú jednotkový prienik.

Majme grupu H danú prezentáciou:

$$H := \left\langle R, (RR') | R^2 = (RR')^a = \underbrace{(RRR')^2}_{=R'^2} = 1 \right\rangle.$$

Je zrejmé, že je to prezentácia dihedrálnej grupy D_{2a} a že obsahuje všetky slová, v ktorých sa nachádzajú iba prvky R a R'. Dokázali sme, že grupa D_{2a} je podgrupou grupy $pmm_1(a,b)$. Teraz dokážeme, že je normálna.

Majme prvok g patriaci do grupy $pmm_1(a,b)$. Máme dokázať, že platí nasledujúca rovnosť: $gHg^{-1} = H$. Ak g patrí do H, tak to zrejme platí, nech teda do D_{2a} nepatrí. Prvok g je však slovo zložené z prvkov R, R', R_2, Y. Keďže z prezentácie vyplýva, že prvok R s R_2 a Y komutuje a taktiež prvok R' komutuje s Y a R_2, môžeme prvok g zapísať ako súčin: $g'h$, kde g' je slovo tvorené prvkami R_2 a Y a h je slovo tvorené prvkami R a R'. Keďže grupa H je generovaná prvkami R a $\underbrace{R'}_{RRR'=R'}$, potom $h \in H$. Teda:

$gHg^{-1} = g'hHh^{-1}g'^{-1} = g'Hg'^{-1} = \left\{ g'h'g'^{-1}; h \in H \right\} = H.$

Posledná rovnosť vyplýva z toho, že prvok g' komutuje s každým prvkom grupy H. Týmto sme ukázali, že D_{2a} je normálnou podgrupou grupy $pmm_1(a,b)$.

Vezmime si teraz grupu G danú prezentáciou:

$$G := \langle R_2, Y | R_2^2 = Y^b = (R_2Y)^2 = 1 \rangle .$$

Táto prezentácia nám udáva dihedrálnu grupu D_{2b}. To, že je to normálna podgrupa grupy $pmm_1(a,b)$ dokážeme analogicky ako v predchádzajúcich riadkoch.

Všetky slová tvorené len písmenami R, R' sa nachádzajú v podgrupe H a všetky slová tvorené R_2, Y sa nachádzajú v podgrupe G. Ukázali sme si, že každý prvok podgrupy H komutuje s každým prvkom podgrupy G, potom vďaka tomu, že iné generátoty ako R, R', Y, R_2 grupa $pmm_1(a,b)$ nemá, bude $pmm_1(a,b) \subseteq H \times G$. Rád grupy $pmm_1(a,b)$ je ale podľa $[I.]$ $4ab$ a rád grupy $H \times G$ je tiež $4ab$, potom prienik podgrúp H a G musí byť triviálny a platí $pmm_1(a,b) \cong D_{2a} \times D_{2b}$.
čbtd

Priamym dôsledkom predchádzajúcej vety je aj veta o počte involúcií.

Dôsledok 6.1 *Grupa $pmm_1(a,b)$ daná prezentáciou (22) má*

1. $a + ab + b$ *involúcií, ak a a b sú nepárne,*
2. $a + ab + 2b + 1$ *involúcií, ak a je párne a b nepárne,*
3. $2a + ab + b + 1$ *involúcií, ak a je nepárne a b je párne a*
4. $2a + ab + 2b + 3$ *involúcií, ak a a b sú párne.*

Na základe predchádzajúcich dvoch viet už vieme vysloviť vetu o izomorfizmoch dvoch grúp $pmm_1(a,b)$ a $pmm_1(a',b')$.

Veta 6.2 *Grupy $pmm_1(a,b)$ a $pmm_1(a',b')$ sú izomorfné jedine vtedy ak*

- $(a,b) = (a',b')$ *alebo* $(a,b) = (b',a')$ *alebo*
- $(a,b) = (2b', \frac{a'}{2})$ *alebo* $(a,b) = (\frac{a'}{2}, 2b')$, *ak b' a $\frac{a'}{2}$ sú nepárne alebo*
- $(a,b) = (2a', \frac{b'}{2})$ *alebo* $(a,b) = (\frac{b'}{2}, 2a')$, *ak a' a $\frac{b'}{2}$ sú nepárne.*

Dôkaz:
(„⇐")
Nech $(a,b) = (a',b')$, potom sa jedná o tú istú grupu. Nech $(a,b) = (b',a')$, potom izomorfizmom bude zobrazenie:

$$\begin{aligned} \varphi : pmm_1(a,b) &\longmapsto pmm_1(a',b') \\ \varphi : R &\longrightarrow {R_2}^\star \\ \varphi : RR' &\longrightarrow Y^\star \\ \varphi : R_2 &\longrightarrow R^\star \\ \varphi : Y &\longrightarrow R^\star {R'}^\star . \end{aligned}$$

Musíme overiť, že platia rovnosti $[\varphi(R), \varphi(Y)] = [\varphi(R'), \varphi(Y)] = [\varphi(R_2), \varphi(R)] = [\varphi(R_2), \varphi(R')] = \varphi(R)^2 = \varphi(R')^2 = \varphi(R_2)^2 = \varphi(Y)^b = (\varphi(R)\varphi(R'))^a = (\varphi(R_2)\varphi(Y))^2 = 1$. Keďže $\varphi(R) = {R_2}^\star, \varphi(R') = \varphi(R)\varphi(RR') = {R_2}^\star Y^\star, \varphi(R_2) = R^\star, \varphi(R_2)\varphi(Y) = {R'}^\star$, potom všetky involúcie z prezentácie grupy $pmm_1(a,b)$ sa nám zobrazia na involúcie v prezentácii grupy $pmm_1(a',b')$.

Teraz overíme, či obrazy budú spolu komutovať .

$$\varphi(R)\varphi(Y)\varphi(R)^{-1} = {R_2}^\star R^\star {R'}^\star ({R_2}^\star)^{-1} = R^\star {R'}^\star = \varphi(Y)$$

Využili sme to, že v grupe $pmm_1(a',b')$ platí $[{R_2}^\star, R^\star] = [{R_2}^\star, {R'}^\star] = 1$. Podobne ukážeme aj ostatné.

Teraz ukážeme, že $\varphi(Y)^b = (R^\star R'^\star)^b = (R^\star R'^\star)^{a'} = 1$. Podobne aj $\varphi(RR')^a = (Y^\star)^a = (Y^\star)^{b'} = 1$. Potom φ je homomorfizmus.

Aby sme ukázali, že je to aj izomorfizmus, stačí nám overiť, či je dané zobrazenie bijektívne. Vzhľadom na to, že obe grupy majú veľkosť $4ab$, stačí overiť, či je to surjektívne zobrazenie. Ale vzhľadom na to, že obrazy generátorov sú opäť generátory, potom je to aj surjektívne zobrazenie, potom sú grupy izomorfné.

Nech teraz platí $(a,b) = (2a', \frac{b'}{2})$. Potom hľadaným izomorfizmom bude zobrazenie:

$$\begin{aligned} \psi : pmm_1(a,b) &\longmapsto pmm_1(a',b') \\ \psi : R &\longrightarrow R^\star \\ \psi : RR' &\longrightarrow R_2^\star R^\star R'^\star \\ \psi : R_2 &\longrightarrow R_2^\star \\ \psi : Y &\longrightarrow R^\star Y^\star. \end{aligned}$$

To, že ψ je skutočne izomorfizmom, by sme overili analogicky ako v predchádzajúcom prípade.

Nech $(a,b) = (\frac{a'}{2}, 2b')$. Potom ale izomorfizmom bude zobrazenie ψ^{-1}. Nech sa teraz $(a,b) = (2b', \frac{a'}{2})$. Potom funkciou izomorfizmu μ bude zobrazenie podobné ψ, ale $R^\star$ sa vo všetkých predpisoch zamení za $R_2^\star$ a podobne $(R^\star R'^\star)$ sa zamení za $Y^\star$. A nakoniec, nech $(a,b) = (\frac{b'}{2}, 2a')$, potom funkciou izomorfizmu bude zobrazenie μ^{-1}, vzhľadom na to, že μ je izomorfizmus, bude bijektívnym homomorfizmom aj μ^{-1}.

(„⇒")

Nech sú grupy $pmm_1(a,b)$ a $pmm_1(a',b')$ izomorfné.

I. Nech a aj b sú nepárne. Potom má grupa $pmm_1(a,b)$ $a+ab+b$ involúcií. Vzhľadom na to, že sú dané grupy izomorfné a ich rády sa musia rovnať, dostávame $4ab = 4a'b'$, čiže $ab = a'b'$. Súčin ab je ale nepárny, potom aj $a'b'$ je nepárny súčin, z čoho vyplýva, že ak sú grupy $pmm_1(a,b)$ a $pmm_1(a',b')$ izomorfné, potom musia byť aj a' a b' nepárne. Počty involúcií sa musia rovnať, z čoho $a + ab + b = a' + a'b' + b'$, odkiaľ po dosadení rovnosti $ab = a'b'$ dostávame $a + b = a' + b'$. Po využití oboch rovností dostávame vzťah: $a'b' - a'b - b'b + b^2 = 0$. Riešme to ako kvadratickú rovnicu s neznámou b. Dostaneme, že $b = a'$ alebo $b = b'$. Odtiaľ už dostávame, že $(a,b) = (a',b')$ alebo $(a,b) = (b',a')$.

II. Nech je a párne a b nepárne. Potom musí byť párne alebo a' alebo b'.

   a) Nech je párne a' a b' je nepárne. Potom, vzhľadom na rovnosť počtu involúcií, dostávame: $a+ab+2b+1 = a'+a'b'+2b'+1$. Využitím rovnosti rádov grúp dostávame: $a+2b = a'+2b'$. Znovu, využitím rovnosti rádov grúp dostávame kvadratickú rovnicu s neznámou b tvaru $2b'^2 - b'(2b+a) + ab = 0$, ktorej riešením je $b' = b$ alebo $b' = \frac{a}{2}$. Teda, v takomto prípade bude platiť: $(a,b) = (a',b')$ alebo $(a,b) = (2b', \frac{a'}{2})$.

   b) Nech sú párne aj a' aj b'. V grupe $pmm_1(a',b')$ potom bude $2a' + ab + 2b' + 3$ involúcií, v grupe $pmm_1(a,b)$ ich bude $a + ab + 2b + 1$. Opäť využívame rovnosť rádov grúp, z čoho dostávame rovnicu: $2a' + 2b' + 2 = a + 2b*$. Vyjadrime a' z rovnice $ab = a'b'$, teda $a' = \frac{ab}{b'}$. Po dosadení do rovnice $*$ dostávame kvadratickú rovnicu tvaru $2ab + 2b'^2 = b'(a + 2b - 2)$. Vyjadrime si diskriminant: $D = (a+2b-2)^2 - 16ab = a^2 - 12ab + 4b^2 - 4a - 8b + 4$. Nech je tento diskriminant nezáporný. Aby bolo b' celé číslo, musí platiť $4|(a + 2b - 2 \pm \sqrt{D})$. Vzhľadom na to, že $4|a'b'$, musí aj $4|ab$, ale keďže je b nepárne, potom $4|a$. Potom $4|(a+2b-2)$, teda aby bol celý výraz deliteľný 4, musí $4|\sqrt{D}$ a teda $16|D$, čo však neplatí, teda v takomto prípade nebudú $pmm_1(a,b)$ a $pmm_1(a',b')$ nikdy izomorfné.

   c) Nech a' je nepárne a b' je párne. Potom postupujeme analogicky ako v bode a). Dostávame kvadratickú rovnicu $2a'^2 - a'(a+2b) + ab = 0$, ktorej riešením vzhľadom na a' je $\frac{a}{2}$ alebo b. Teda $(a,b) = (2a', \frac{b'}{2})$ alebo $(a,b) = (b',a')$.

III. Nech je teraz a nepárne a b párne. Postupovať budeme rovnako ako v bode II., ale všade preznačíme a za b a naopak b za a. Dostávame, že ak sú grupy $pmm_1(a,b)$ a $pmm_1(a',b')$ izomorfné, potom $(a,b)=(a',b')$ alebo $(a,b)=(\frac{a'}{2},2b')$ alebo $(a,b)=(\frac{b'}{2},2a')$ alebo $(a,b)=(b',a')$.

IV. Nech sú a aj b párne. Izomorfizmy s grupami, kde sú parametre rôznej parity sme vyriešili v predchádzajúcich 2 bodoch, ostáva nám prípad, keď a' aj b' budú párne. Ale aj tu nakoniec dostávame kvadratickú rovnicu tvaru $a'b'-a'b-b'b+b^2=0$, čo je ale rovnica z prípadu I.

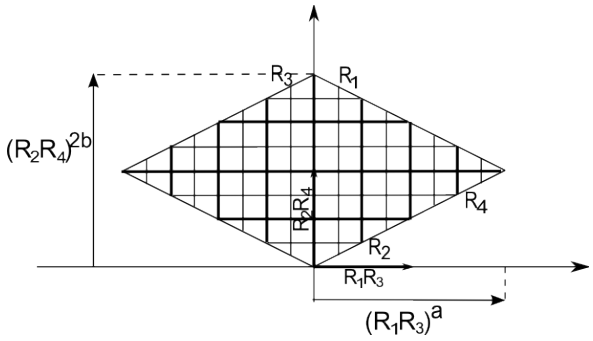
čbtd

6.2 Štrukturálne vlastnosti grupy $pmm_2(a,b)$

Ďalšou grupou je $pmm_2(a,b)$. Daná je nasledujúcim predpisom:

$$\begin{aligned} pmm_2(a,b) := \langle R_1,R_2,R_3,R_4 | R_1^2=R_2^2=R_3^2=R_4^2=[R_1,R_2]= \\ [R_1,R_4]=[R_2,R_3]=[R_3,R_4]=(R_1R_3)^a(R_2R_4)^b=(R_2R_4)^{2b}=1\rangle. \end{aligned} \tag{23}$$

Predstavu, ako grupa $pmm_2(a,b)$ vyzerá, nám dáva obrázok (14)



Obrázok 14: Grupa $pmm_2(a,b)$

Znovu si odvodíme všeobecný tvar prvku.

Veta 6.3 *Každý prvok grupy $pmm_2(a,b)$ určenej prezentáciou (23) má kanonický tvar:*

$$R_1^i(R_1R_3)^j(R_2R_4)^kR_4^l, \tag{24}$$

kde $i,l\in\{0,1\}$, $j\in\{0,1,...,a-1\}$ a $k\in\{0,1,...,2b-1\}$.

Dôkaz: Každý prvok ľubovoľnej grupy je postupnosťou jej generátorov a naopak. To znamená v našej grupe každá postupnosť tvaru: $R_1^{i_1}R_2^{j_1}R_3^{k_1}R_4^{l_1}R_1^{i_2}R_2^{j_2}...$ určuje nejaký prvok grupy $pmm_2(a,b)$. Keďže všetky jej generátory sú involúcie, potom nám stačí uvažovať $i_n,j_n,k_n,l_n\in\{0,1\}$ pre ľubovoľné n. Z prezentácie (23) vyplýva, že R_1 komutuje s R_2 a s R_4 a prvok R_3 komutuje s R_2 a R_4. T.z. že môžeme prvky R_1 a R_3 presunúť do prvej polovice postupnosti a v druhej ostanú len prvky R_2 a R_4. Dostávame prvok tvaru $R_1^{i'}(R_1R_3)^{j'}R_1^{i''}R_4^{l'}(R_2R_4)^{k'}R_4^{l''}$, kde $i',i'',l',l''\in\{0,1\}$ a j' a k' sú ľubovoľné.

Vyjadrime si, čomu sa rovná nasledujúci výraz: $R_1^l(R_1R_3)^jR_1^l$. Ak $l=0$, potom $R_1^0(R_1R_3)^jR_1^0=(R_1R_3)^j=(R_1R_3)^{(-1)^0j}$. Ak $l=1$, potom $R_1^1(R_1R_3)^jR_1^1=(R_3R_1)^j=(R_1R_3)^{-1}=(R_1R_3)^{(-1)^1j}$.

Teraz už môžeme pokračovať:
$R_1^{i'}(R_1R_3)^{j'}R_1^{i''}R_4^{l'}(R_2R_4)^{k'}R_4^{l''}=R_1^{i'}R_1^{i''}R_1^{i''}(R_1R_3)^{j'}R_1^{i''}R_4^{l'}(R_2R_4)^{k'}R_4^{l'}R_4^{l'}R_4^{l''}=$
$=\underbrace{R_1^{i'+i''}}_{R_1^i}\underbrace{(R_1R_3)^{(-1)^{i''}j'}}_{(R_1R_3)^j}\underbrace{(R_2R_4)^{(-1)^{l'}k'}}_{(R_2R_4)^k}\underbrace{R_4^{l'+l''}}_{R_4^l}$. Z prezentácie (23) vieme, že $(R_1R_3)^a=(R_2R_4)^{-b}=$

$(R_2R_4)^b$. Poslednú rovnosť sme si mohli dovoliť písať vďaka tomu, že $(R_2R_4)^b$ je involúcia. Ďalej postupujeme podobne ako vo vete o štruktúre prvku grupy $pm_2(a,b)$.

Vzhľadom na to, že veľkosť grupy je $4ab$(vyplýva z článku [1.]), daný tvar je jednoznačne určený. **čbtd**

Cestou k odpovedi, kedy sú dve grupy $pmm_2(a,b)$ a $pmm_2(a',b')$ je znovu počet involúcií. Najprv si ale odvoďme, ako vyzerá všeobecný súčin dvoch ľubovoľných prvkov.

Príklad 6.1 Majme prvky $R_1^i(R_1R_3)^j(R_2R_4)^kR_4^l$ a $R_1^{i'}(R_1R_3)^{j'}(R_2R_4)^{k'}R_4^{l'}$ patriace do grupy $pmm_2(a,b)$, kde $i,i',l,l' \in \{0,1\}$, $j,j' \in \{0,1,...,a-1\}$ a $k,k' \in \{0,1,...,2b-1\}$. Potom prvok:

$$R_1^i(R_1R_3)^j(R_2R_4)^kR_4^lR_1^{i'}(R_1R_3)^{j'}(R_2R_4)^{k'}R_4^{l'} = R_1^i(R_1R_3)^jR_1^{i'}(R_1R_3)^{j'}(R_2R_4)^kR_4^l(R_2R_4)^{k'}R_4^{l'} =$$

$$= R_1^{i+i'}(R_1R_3)^{(-1)^{i'}j+j'}(R_2R_4)^{k+(-1)^lk'}R_4^{l+l'}.$$

Veta 6.4 *V grupe $pmm_2(a,b)$ je:*

a) $2(a+ab+b)+1$ *involúcií, ak a alebo b je nepárne,*

b) $2(a+ab+b)+3$ *involúcií, ak a aj b sú párne.*

Dôkaz: V predchádzajúcom príklade sme si odvodili, ako vyzerá všeobecný súčin dvoch prvkov. Ak budeme medzi sebou násobiť rovnaký prvok, dostaneme:
$R_1^i(R_1R_3)^j(R_2R_4)^kR_4^lR_1^i(R_1R_3)^j(R_2R_4)^kR_4^l = R_1^{i+i}(R_1R_3)^{(-1)^ij+j}(R_2R_4)^{k+(-1)^lk}R_4^{l+l}$. Keďže rád prvkov R_1 a R_2 je 2, potom druhá mocnina ľubovoľného prvku $R_1^i(R_1R_3)^j(R_2R_4)^kR_4^l$ bude $(R_1R_3)^{(-1)^ij+j}(R_2R_4)^{k+(-1)^lk}$. Vo vete o štruktúre prvku grupy $pmm_2(a,b)$ sme si dokázali, že je to jednoznačný zápis a ak má platiť: $(R_1R_3)^{(-1)^ij+j}(R_2R_4)^{k+(-1)^lk} = 1$, musia platiť nasledujúce rovnosti:

$$(-1)^ij + j \equiv 0 \pmod{a}$$
$$(-1)^lk + k \equiv 0 \pmod{2b}.$$

Vzhľadom na to, že $j \in \{0,1,...,a-1\}$ a $k \in \{0,1,...,2b-1\}$ sa nám rovnice redukujú na nasledjúce 4: $(-1)^ij + j = 0$ alebo $(-1)^ij + j = a$ a $(-1)^lk + k = 0$ alebo $(-1)^lk + k = 2b$.

a) Nech a je nepárne. Nech $i = 1$. Potom pre prvú rovnicu je riešením každé j a naopak, druhá rovnica riešenie nemá. Podobne pre $l = 1$ má tretia rovnica riešenie pre každé k a v stvrtá pre žiadne. Nech i alebo l je 0. Potom pre prvú rovnicu je riešením jedine číslo $j = 0$ a druhá riešenie nemá, keďže a je nepárne. Z tretej rovnice dostávame výsledok $k = 0$ a zo štvrtej $k = b$. Ak to zhrnieme, máme dokopy $2ab + 2b + 2a + 2$ involúcií, medzi ktorými sa ale nachádza aj jednotkový prvok.

b) Nech a je párne. $2ab + 2a + 2b + 1$ involúcií dostaneme analogický ako v prípade a). V tomto prípade ale pre $i = 0$ má aj druhá rovnica riešenie a to $j = \frac{a}{2}$. Potom $(R_1R_3)^{(-1)^ij+j}(R_2R_4)^{k+(-1)^lk} = (R_1R_3)^a(R_2R_4)^{k+(-1)^lk} = (R_2R_4)^{k+(-1)^lk+b} = 1$. Z toho vyplýva, že $k + (-1)^lk + b = 0$ alebo $k + (-1)^lk + b = 2b$ alebo $k + (-1)^lk + b = 4b$. Vzhľadom na to, že k je nezáporne celé číslo a b je kladné, prvá rovnica riešenie mať nebude. Druhá bude mať jedine v prípade, že $l = 0$, potom $k = \frac{b}{2}$. Rovnako tretia rovnica bude mať riešenie jedine pre nulové l a párne b, potom $k = \frac{3b}{2}$.

čbtd

Vďaka tomu, že poznáme v jednotlivých grupách $pmm_2(a,b)$ počty involúcií, vieme povedať, kedy dve grupy $pmm_1(a,b)$ a $pmm_2(a',b')$ budú izomorfné.

Veta 6.5 *Grupy $pmm_2(a,b)$ a $pmm_2(a',b')$ sú izomorfné práve vtedy, keď $(a,b) = (a',b')$ alebo $(a,b) = (b',a')$.*

Dôkaz:

(„⇒")

Dôkaz si rozdelíme na 2 časti.

I. Nech a alebo b je nepárne. Potom má grupa $pmm_2(a,b)$ $2(a+ab+b)+1$ involúcií.

a) Nech a' alebo b' je nepárne, potom má grupa $pmm_2(a',b')$ $2(a'+a'b'+b')+1$ involúcií. Podľa článku [1.] má grupa $pmm_2(a,b)$ $8ab$ prvkov. Z predpokladu, že sú grupy $pmm_2(a,b)$ a $pmm_2(a',b')$ izomorfné, musí platiť $ab = a'b'(1)$. Využitím tejto rovnosti a úpravami dostávame rovnicu tvaru $a+b = a'+b'$. Vyjadrime s a' z rovnice (1), teda $a' = \frac{ab}{b'}$. Dosadením dostávame kavdratickú rovnicu ${b'}^2 - b'(a+b)+ab = 0(2)$. Po vyriešení $b' = a$ alebo $b' = b$.

b) Nech sú a' aj b' párne, potom počet involúcií v grupe $pmm_2(a',b')$ je $2(a'+a'b'+b')+3$. Využitím podobných úvah ako v predchádzajúco bode, dostávame kvadratickú rpvnicu ${b'}^2 - b'(a+b-1)+ab = 0$. Diskriminant tejto rovnice po úpravách je $b^2 - 2b(a-3) + (a-1)^2(3)$. Aby b' bolo celé číslo, musí byť celá aj odmocnina z diskriminantu. Teda, diskriminant musí byť druhou mocninou nejakého čísla, teda diskriminant rovnice (3) musí byť rovný nule. Ten je ale rovný číslu $4(a-3)^2 - 4(a-1)^2$, čo pre $a > 2$ je záporné číslo. Ak a' aj b' sú párne a a alebo b je nepárne, potom musí platiť $4|a$ alebo $4|b$ (alebo sa v tomto prípade berie vo vylučovacom význame). Ak $4|a$, potom $4 \leq a$, ale v tom prípade bude diskriminant záporný, potom musí platiť $4|b$, tým pádom je a nepárne, čiže musí platiť $a = 1$. Rovnica (3) sa zjednoduší na tvar $b^2 + 4b = 0$. V tomto prípade ale b nebude celé číslo, teda v takomto prípade grupy $pmm_2(a,b)$ a $pmm_2(a',b')$ izomorfné nie sú.

II. Nech a aj b sú párne, potom má grupa $pmm_2(a,b)$ $2(a+ab+b)+3$ involúcií.

c) Nech a' alebo b' je nepárne. Potom budeme postupovať rovnako ako v bode $I.b)$, len preznačíme a za a', b za b'. Tam sme dokázali, že ak sú grupy $pmm_2(a,b)$ a $pmm_2(a',b')$ izomorfné, potom takýto prípad nemôže nastať.

d) Nech sú a' aj b' párne. Potom v grupe $pmm_2(a',b')$ je $2(a'+a'b'+b')+3$ involúcií. Jednoduchými úpravami dostávame opäť rovnicu (1) a odtiaľ kvadratickú rovnicu (2), teda ak sú grupy $pmm_2(a,b)$ a $pmm_2(a',b')$ izomorfné, potom platí $(a,b) = (a',b')$ alebo $(a,b) = (b',a')$.

(„⇐")

Nech platí $(a,b) = (a',b')$. Potom sa jedná o totožné grupy. Nech $(a,b) = (b',a')$, potom vezmime zobrazenie

$$\begin{aligned} \varphi : pmm_2(a,b) &\longmapsto pmm_2(a',b) \\ \varphi : R_1 &\longmapsto R_2' \\ \varphi : R_2 &\longmapsto R_1' \\ \varphi : R_3 &\longmapsto R_4' \\ \varphi : R_4 &\longmapsto R_3'. \end{aligned}$$

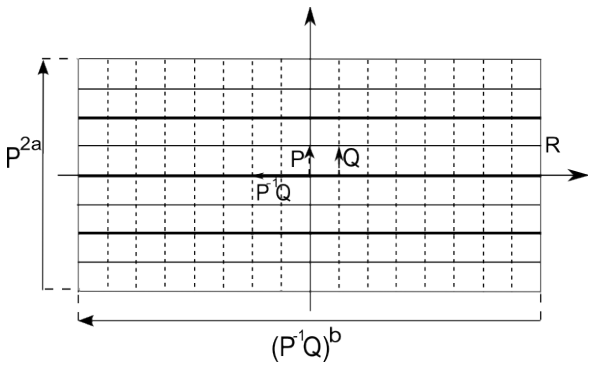
Vzhľadom na to, že zobrazujeme generátory jednej grupy na generátory druhej grupy, bude to surjektívny homomorfizmus. Využitím rovnosti rádov grúp dostávame, že to je izomorfizmus.
čbtd

6.3 Štrukturálne vlastnosti grupy $pmg_1(a,b)$

Grupa $pmg_1(a,b)$ znázornená na obrázku (15) je daná prezentáciou:

$$pmg_1(a,b) := \left\langle P,Q,R | P^2 = Q^2, R^2 = (RP)^2 = (RQ)^2 = P^{2a} = (P^{-1}Q)^b = 1 \right\rangle. \tag{25}$$

Pozrime sa na to, ako vyzerá kanonický tvar prvku.



Obrázok 15: Grupa $pmg_1(a,b)$

Veta 6.6 *Každý prvok grupy $pmg_1(a,b)$ je daný nasledujúcim kanonickým tvarom:*

$$R^i(P^2)^j(P^{-1}Q)^kP^l, \tag{26}$$

kde $i \in \{0,1\}$, $j \in \{0,1,...,a-1\}$, $k \in \{0,1,...,b-1\}$ a $l \in \{0,1\}$.

Dôkaz: V grupe $pmg_1(a,b)$ je podgrupou grupa $H := \langle P,Q|P^2 = Q^2, P^{2a} = (P^{-1}Q)^b = 1\rangle$. Prezentácia podgrupy H je ale predpisom pre grupu $pg_1(b,a)$, ktorej veľkosť je $2ab$ a veľkosť grupy $pmg_1(a,b)$ je $4ab$, potom H je podgrupa indexu 2. Môžeme písať $pmg_1(a,b) = pg_1(a,b) \cup R.pg_1(a,b)$. Prvok grupy $pmg_1(a,b)$ je teda vyjadrený ako súčin nejakej mocniny R a ľubovoľného prvku patriaceho do $pg_1(a,b)$.
čbtd

Grupy $pg_1(a,b)$ a $pg_1(a',b')$ sú izomorfné jedine v prípade, že $a = a'$ a $b = b'$. V grupe $pmg_1(a,b)$ však vieme nájsť aj iné izomorfné grupy. Najprv si ukážeme počet involúcií.

Veta 6.7 *Grupa $pmg_1(a,b)$ má*

1. *$ab + 2b + 3$ involúcií, ak oba parametre sú párne,*
2. *$ab + 2b + a + 1$ involúcií, ak a je párne a b nepárne,*
3. *$ab + b + 1$ involúcií, ak a je nepárne a b je párne a*
4. *$ab + a + b$ involúcií, ak oba parametre sú nepárne.*

Dôkaz: Ako bolo v predchádzajúcom povedané, v grupe $pmg_1(a,b)$ existuje podgrupa $pg_1(a,b)$ a teda všetky involúcie grupy $pg_1(a,b)$ sú involúciami grupy $pmg_1(a,b)$ a tých je v prípade 1. 3, v prípade 2. ich je $a+1$, v 3. je 1 involúcia a v poslednom prípade je v $pg_1(a,b)$ a involúcií.

Teraz nájdeme involúcie v množine $R.pg_1(a,b)$. Taký prvok je tvaru $R(P^2)^j(P^{-1}Q)^kP^l$. Aby bol involúciou, musí platiť $R(P^2)^j(P^{-1}Q)^kP^lR(P^2)^j(P^{-1}Q)^kP^l = 1$.

$$1 = R(P^{-1}Q)^kP^lR(P^{-1}Q)^kP^l$$

tu sme využili fakt, že v grupe $pg_1(a,b)$ patrí P^2 do centra a následne z prezentácie vieme, že $PRP = R$

$$= R(P^{-1}Q)^kRP^{-l}(P^{-1}Q)^kP^l$$

opäť využívame fakt, že $PRP = R$

$$= R(P^{-1}Q)^kR(P^{-1}Q)^{(-1)^lk}$$

v príklade 5.2 sme si ukázali, že $P^l(P^{-1}Q)^kP^{-l} = (P^{-1}Q)^{(-1)^lk}$, ukážeme, že to platí aj pre $P^{-l}(P^{-1}Q)^kP^l$, ak $l = 0$, potom to platí, ak $l = 1$, potom $P^{-1}(P^{-1}Q)^kP = Q^{-1}(P^{-1}Q)^{k-1}P = (Q^{-1}P)^k = (P^{-1}Q)^{(-1)^lk}$

$$= (P^{-1}Q)^{(-1)^lk+k}$$

tu sme využili, že $PRP = QRQ = R$ a teda $P^{-1}QRQP^{-1} = P^{-1}QR(PQ^{-1})^{-1} = P^{-1}QR(P^{-1}Q)^{-1} = R$ a následne $R^2 = 1$. Vzhľadom na to, že v podgrupe $pg_1(a,b)$ je prvok jednoznačne daný, vieme, že $(-1)^lk + k = 0(1)$ alebo $(-1)^lk + k = a(2)$. Ak $l = 1$, potom rovnica (1) platí pre všetky k a j, (2) pre žiadne. Ak $l = 0$, potom (1) platí pre každé j a pre $k = 0$ a rovnica (2) platí pre každé j a pre $k = \frac{a}{2}$. Teda, ak to zhrnieme, v prípade, že a je párne, je v množine $R.pg_1(a,b)$ $ab + 2b$ involúcií, ak a je nepárne, potom je v nej $ab + b$ involúcií.

V prvom prípade teda máme dokopy $ab + 2b + 3$ involúcií, v druhom ich je $ab + 2b + a + 1$, v treťom $ab + b + 1$ a v poslednom prípade je $ab + b + a$ involúcií.

čbtd

Veta 6.8 *Grupy $pmg_1(a,b)$ a $pmg_1(a',b')$ sú izomorfné práve vtedy, keď*

a) $(a,b) = (a',b')$,

b) $(a,b) = (b',a')$, *keď* a,b,a',b' *sú nepárne,*

c) $(a,b) = (2b', \frac{a'}{2})$, *ak* a,a' *sú párne a* b,b' *sú nepárne.*

Dôkaz:

(„⇐")

Nech platí a). Potom sa jedná o totožné grupy. Nech platí b). Vezmime predpis:

$$\varphi : pmg_1(a,b) \longmapsto pmg_1(a',b')$$
$$\varphi : P \longmapsto R'P'^{-1}Q'$$
$$\varphi : Q \longmapsto R'P'Q'$$
$$\varphi : R \longmapsto P'^{a'}.$$

Najprv musíme ukázať, že φ je homomorfizmus. Musí platiť
$\varphi(1) = \varphi(P)^2\varphi(Q)^{-2} = (\varphi(R)\varphi(P))^2 = (\varphi(R)\varphi(Q))^2 = \varphi(P)^{2a} = (\varphi(P)^{-1}\varphi(Q))^b = 1$. Využívajúc relácie z prezentácie (25) dostávame:

$$\varphi(1) = \varphi(P^2Q^{-2}) = \varphi(P)^2\varphi(Q)^{-2} = R'P'^{-1}Q'R'P'^{-1}Q'(R'P'Q')^{-2} =$$
$$= P'Q'^{-1}P'^{-1}Q'Q'^{-1}P'^{-1}R'Q'^{-1}P'^{-1}R' = P'^{-1}Q'^{-1}Q'P' = 1$$

v tomto bode sme opakovane využili $R'P'R' = P'^{-1}$ a tiež $R'Q'R' = Q'^{-1}$, rovnako z prezentácie $P'^2 = Q'^2$ a tiež, že v podgrupe $pg_1(b,a)$ patrí prvok P'^2 do centra

$$= \varphi((RP)^2) = (\varphi(R)\varphi(P))^2 = (P'^{a'}R'P'^{-1}Q')^2 =$$
$$= R'P'^{-a'-1}Q'P'^{a'}R'P'^{-1}Q' = R'Q'P'^{-a'-1}P'^{a'}R'P'^{-1}Q' = R'Q'P'^{-1}R'P'^{-1}Q' =$$
$$= Q'^{-1}P'P'^{-1}Q' = 1$$

využili sme, že a' je nepárne, potom $P'^{-a'-1}$ patrí do centra

$$= \varphi((RQ)^2) = (\varphi(R)\varphi(Q))^2 = P'^{a'}R'P'Q'P'^{a'}R'P'Q' = R'P'^{-a'+1}Q'P'^{a'}R'P'Q' =$$
$$= R'Q'P'R'P'Q' = Q'^{-1}P'^{-1}P'Q' = 1$$
$$= \varphi(P^{2a}) = (\varphi(P)^2)^a = (R'P'^{-1}Q'R'P'^{-1}Q')^a = (P'Q'^{-1}P'^{-1}Q')^a = (P'^{-1}Q')^{2a} =$$
$$= (P'^{-1}Q')^{2b'} = ((P'^{-1}Q')^{b'})^2 = 1^2 = 1$$
$$= \varphi((P^{-1}Q)^b) = (\varphi(P)^{-1}\varphi(Q))^b = (Q'^{-1}P'R'R'P'Q')^b = (Q'^{-1}P'^2Q')^b = P'^{2b} = P'^{2a'} = 1.$$

Dokázali sme, že φ je skutočne homomorfizmus, teraz ukážeme, že je to surjektívne zobrazenie. Keďže $Im(\varphi)$ je podgrupou, musia tam patriť aj prvky $\varphi(P)^{-1}\varphi(Q) = P'^2$, $P'^{2.\frac{a'+1}{2}}P'^{-a'} = P'$, $\varphi(P)^2 = P'^{-1}Q'$, potom aj $P'P'^{-1}Q' = Q'$ a napokon $R'P'Q'Q'^{-1}P'^{-1} = R'$. Keďže grupa $Im(\varphi)$ obsahuje ako svoje prvky generátory grupy $pmg_2(a,b)$, potom sa grupy $Im(\varphi)$ a $pmg_1 9a,b)$ budú rovnať a zobrazenie je surjektívne. Keďže $ab = a'b'$, potom bude aj injektívne a φ bude izomorfizmom.

Majme teraz prípad c). Dokážeme, že nasledujúci predpis bude izomorfizmom medzi grupou $pmg_1(a,b)$ a $pmg_1(a',b')$.

$$\psi : pmg_1(a,b) \longmapsto pmg_1(a',b')$$
$$\psi : P \longmapsto R'P'^{\frac{a'}{2}}P'^{-1}Q'$$
$$\psi : Q \longmapsto R'P'^{\frac{a'}{2}}P'Q'$$
$$\psi : R \longmapsto P'^{a'}$$

To, že ψ je skutočne bijektívny homomorfizmus ukážeme analogicky ako v predchádzajúcom prípade.

(„⇒")

Nech sú grupy $pmg_1(a,b)$ a $pmg_1(a',b')$ izomorfné. Potom sa ich počty involúcií a ich rády musia rovnať. Odtiaľ bude platiť $ab = a'b'(1)$.

I. Nech a aj b sú nepárne. Potom počet involúcií v grupe $pmg_1(a,b)$ je $ab + a + b$.

   a) Ak sú nepárne aj a' aj b', potom dostávame rovnicu $a + b = a' + b'$, využitím rovnosti $ab = a'b'$, dostávame riešenie $a = a'$ alebo $a = b'$.

   b) Iné prípady vzhľadom na to, že $ab = a'b'$ nastať nemôžu, pretože na ľavej strane je nepárny výraz a na pravej by už bol párny.

II. Nech a aj b sú párne, potom počet involúcií v grupe $pmg_1(a,b)$ je $ab + 2b + 3$.

   c) Ak aj a', b' sú párne, potom $ab + 2b + 3 = a'b' + 2b' + 3$. Jediným riešením tejto rovnice využitím (1) je $b = b'$.

   d) Ak a' je párne a b' je nepárne, potom v grupe $pmg_1(a',b')$ je $a'b' + 2b' + a' + 1$ involúcií. Pomocou jednoduchých úprav a využitím (1) dostávame kvadratickú rovnicu $2b'^2 - b'(2b+2) + ab = 0$. Diskriminant tejto rovnice je $4b^2 + 8b(1-a) + 4(2)$. Aby bolo číslo b' celé, musí byť aj odmocnina z diskriminantu celá, teda musí byť druhou mocninou nejakého čísla. Preto sa musí determinant rovnice (2) rovnať nule. Determinantom je číslo $a^2 - 2a + 48$ rovnajúce sa nule. Lenže taká rovnica v obore reálnych čísel riešenie nemá, preto v takomto prípade nebudú grupy $pmg_1(a,b)$ a $pmg_1(a',b')$ nikdy izomorfné.

   e) Nech a' je nepárne a b' je párne, potom je v grupe $pmg_1(a',b')$ $a'b' + b' + 1$ involúcií. Využitím rovnosti počtu involúcií a (1) dostávame rovnosť $2(b+1) = b'$. Keďže je b párne, potom ľavú stranu delí dvojka, ale štvorka nie. Keďže štvorka delí súčin $a'b'$ a a' je nepárne, potom musí deliť b', čo je ale spor.

III. Nech a je párne a b nepárne. Počet involúcií je v tomto prípade $ab + 2b + a + 1$.

   f) Ak a', b' sú párne, potom sa jedná o prípad IId), len sú preznačené a za a' a b za b' a naopak.

   g) Nech a' je párne a b' nepárne. Potom dostávame kvadratickú rovnicu $2b'^2 - b'(2b+a) + ab = 0$. Jej riešeniami sú čísla $b' = b$ alebo $b' = \frac{a}{2}$.

   h) Nech a' je nepárne a b' je párne. Potom $2b + a = b'$, čiže $a' = \frac{ab}{2b+a}$. Nech $2|a$, ale štvorka nedelí a. Potom $\frac{ab}{2b+a} = \frac{2.(2k+1)(2l+1)}{2(2l+1+2k+1)} = \frac{2n+1}{2m}$, kde $b = 2l+1$, $a = 2(2k+1)$, $n = 2kl+k+l$ a $m = l + k + 1$. Keďže menovateľ je párny a čitateľ nepárny, potom a' nie je celé číslo.

Nech $4|a$, potom $a' = \frac{4k(2l+1)}{2(2l+1+2k)} = \frac{2k(2l+1)}{2(k+l)+1}$. Ak toto číslo bude celé, bude párne, ale to je spor.

IV. Nech a je nepárne a b je párne. Potom je v grupe $pmg_1(a,b)$ $ab+b+1$ involúcií.

i) Nech sú a' aj b' párne, potom je to však prípad $II.e$), len a s a' a b s b' sú preznačené a naopak.

j) Nech je a' párne a b' nepárne. Potom sa jedná o prípad $III.h$), len sú znovu parametre preznačené.

k) Nech je a' nepárne a b' párne. Potom dostávame rovnosť $b = b'$.

čbtd

6.4 Štrukturálne vlastnosti grupy $pmg_2(a,b)$

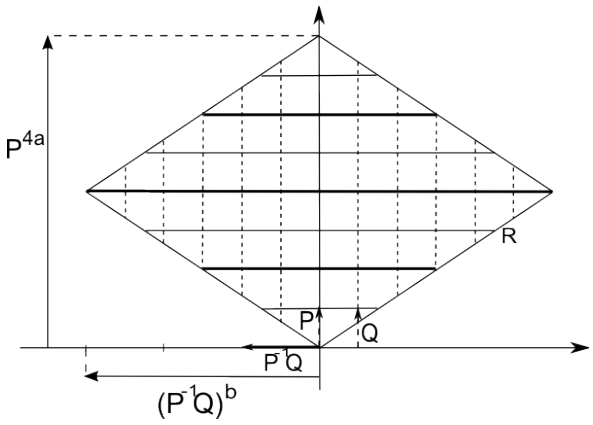
Podobnou grupou ako $pmg_1(a,b)$ je grupa $pmg_2(a,b)$ daná prezentáciou:

$$pmg_2(a,b) := \left\langle P,Q,R | P^2 = Q^2, R^2 = (RP)^2 = (RQ)^2 = P^{4a} = P^{2a}(P^{-1}Q)^b = 1 \right\rangle . \qquad (27)$$

Opäť ako v predchádzajúcom prípade obsahuje grupa $pmg_2(a,b)$ ako svoju podgrupu kvocient grupy pg, v tomto prípade
$\left\langle P,Q | P^2 = Q^2, P^{4a} = P^{2a}(P^{-1}Q)^b = 1 \right\rangle = pg_2(b,a)$. Na obrázku (16) môžeme vidieť, že skutočne sa geometrická interpretácia grupy $pmg_2(a,b)$ od geometrickej interpretácie grupy $pg_2(b,a)$ líši len nepatrne. Z článku [I.] vyplýva, že veľkosť grupy $pmg_2(a,b)$ je $8ab$ a veľkosť grupy $pg_2(b,a)$ je $4ab$, čo znamená, že $pg_2(b,a)$ je podgrupa indexu 2 a teda je to normálna podgrupa. V tomto prípade môžeme vyjadriť grupu $pmg_2(a,b)$ nasledovne:

$$pmg_2(a,b) = \langle R \rangle . pg_2(b,a).$$

Z tohto vzťahu by už automaticky plynul kanonický tvar prvku, keďže sme v stati o grupách pg dokázali, ako vyzerá všeobecný tvar prvku grupy $pg_2(b,a)$.



Obrázok 16: Grupa $pmg_2(a,b)$

Tak ako ani grupy $pg_2(a,b)$ a $pg_2(a',b')$ nie sú izomorfné pre nerovnajúce sa parametre, nie sú izomorfné ani $pmg_2(a,b)$ a $pmg_2(a',b')$. Na dôkaz použijeme počet involúcií.

Veta 6.9 *Grupa $pmg_2(a,b)$ má*

- $2ab+2a+1$ *involúcií, ak a alebo b je nepárne a*

- $2ab + 2a + 3$ *involúcií, ak* a *aj* b *sú párne.*

Dôkaz: Povedali sme si, že každý prvok grupy $pmg_2(a, b)$ je tvaru Rg, kde $g \in pg_2(b, a)$. Musíme ukázať, kedy je prvok $R^i(P^2)^k(P^{-1}Q)^jP^l$ involúciou.

$$\begin{aligned} R^i(P^2)^k(P^{-1}Q)^jP^lR^i(P^2)^k(P^{-1}Q)^jP^l &= R^i(P^2)^k(P^{-1}Q)^jR^iP^{(-1)^il}(P^2)^k(P^{-1}Q)^jP^l \\ &= R^i(P^2)^kR^i(P^{-1}Q)^j(P^2)^kP^{(-1)^il}(P^{-1}Q)^jP^l \end{aligned}$$

Využili se, že $RPRP = 1$, potom $PR = RP^{-1}$, čiže $P^lR^i = R^iP^{(-1)^il}$. Prvky $P^{-1}Q$ a R spolu komutujú, pretože $RP^{-1}QR = PQ^{-1} = P^{-1}Q$. Ďalej sme využili, že v grupe $pg_2(b, a)$ patrí prvok P^2 do centra.

$$= (P^2)^{(-1)^ik}(P^2)^k(P^{-1}Q)^j(P^{-1}Q)^{(-1)^{(-1)^il}j}P^{l+(-1)^il}$$

Znovu sme využívali, že P^2 patrí v $pg_2(b, a)$ do centra a $RP^kR = (RPR)^k = P^{-k}$. Potom sme využili príklad 6.1, kde sme si ukázali, že $P^l(P^{-1}Q)^jP^{-1} = (P^{-1}Q)^{(-1)^lj}$.

$$= (P^2)^{k+(-1)^ik}(P^{-1}Q)^{j+(-1)^lj}P^{l+(-1)^il} = 1$$

Využili sme, že $(-1)^{(-1)^il} = (-1)^l$.
Teraz ukážeme, pre ktoré trojice (k, j, l) bude posledná rovnosť platiť v podgrupe $pg_1(b, a)$(v takom prípade bude $i = 0$) a v množine $R.pg_2(b, a)$(tu $i = 1$).

Nech $i = 0$, spočítame, koľko involúcií má podgrupa $pg_2(b, a)$. Dostávame rovnosť $(P^2)^{2k+l}(P^{-1}Q)^{j+(-1)^lj} = 1$. Potom musí platiť $j + (-1)^lj \equiv 0 \pmod b$. Keďže $0 \leq j < b$, bude platiť rovnosť $j + (-1)^lj = 0$ alebo $j + (-1)^lj = b$.
Nech $l = 1$, potom $j - j = 0$ alebo $j - j = b$. Druhá z rovností v takomto prípade nastať nemôže a prvá platí pre každé j. Potom $(P^2)^{2k+l}(P^{-1}Q)^{j+(-1)^lj} = (P^2)^{2k+1}$, z prezentácie (27) vieme, že $P^{4a} = 1$, potom $4k + 2 \equiv 0 \pmod{4a}$, čo neplatí pre žiadne k, teda pre $l = 1$ nebude v $pg_2(b, a)$ žiadna involúcia.
Nech $l = 0$, potom $2j \equiv 0 \pmod b$, teda $2j = 0$ alebo $2j = b$. Prvá z rovností platí len pre nulové j, v druhej dostávame $j = \frac{b}{2}$, čo je celé číslo len pre párne b. Nech $j = 0$, potom $(P^2)^{2k} = 1$, čo platí len pre $k = 0$ alebo $k = a$. Pri nulovom k by sme ale dostali neutrálny prvok, ktorý je rádu 1, preto v tomto prípade dostávame len 1 involúciu. Nech $j = \frac{b}{2}$, potom $4k + 2a \equiv 4a \pmod{4a}$, potom $2(2k - a) = 4al$ pre nejaké l, čo má riešenie len pre $k = \frac{a}{2}$ alebo $k = \frac{3a}{2}$, čo sú celé čísla len pre párne a. Ak to zhrnieme, ak a alebo b je nepárne, potom je počet involúcií v podgrupe $pg_2(b, a)$ 1, ak a aj b sú párne, potom sú 3.

Nech $i = 1$, potom sa jednotkovému prvku musí rovnať $(P^{-1}Q)^{j+(-1)^lj}$. Ak $l = 1$, potom je prvok tvaru $R(P^2)^k(P^{-1}Q)^jP$ pre každé k, j involúciou, čo je podľa vety 6.8 $2ab$ prvkov. Nech $l = 0$, potom musí platiť $2j \equiv 0 \pmod b$, čo vzhľadom na rozsah výberu čísla j znamená $2j = 0$ alebo $2j = b$. Nech $2j = b$, potom musí byť prvok P^{2a} jednotkou, čo ale podľa geometrickej interetácie z obrázku (16) neplatí. Potom musí platiť $2j = 0$, teda $j = 0$, potom prvok $R(P^2)^k$ je involúciou pre každé k, čo je $2a$ prvkov.

Z predchádzajúcich dvoch odstavcov vieme, že grupa $pmg_2(a, b)$ má pre párne parametre a, b dokopy $2ab + 2a + 3$ involúcií a ak a alebo b je nepárne, potom má grupa $pmg_2(a, b)$ $2ab + 2a + 1$ involúcií.
čbtd

Nielen pri tejto grupe, ale aj v tých nasledujúcich budeme počítať, koľko dvojíc prvkov je na seba kvázikolmých.

Definícia 6.1 *Nech prvky* g *a* h *patria do grupy* G*. Povieme, že prvok* h *je na* g *kvázikolmý, ak platí rovnosť:*

$$hgh^{-1} = g^{-1}. \tag{28}$$

Poznámka: V geometrii platí, že ak je zobrazenie h kolmé na zobrazenie g, potom je aj g kolmé na h. Taktiež platí, že ak h je zobrazenie kolmé samo na seba, potom je to identické zobrazenie. V tomto prípade však symetrickosť všeobecne neplatí a sama na seba môže byť kolmá aj involúcia, preto označenie kvázikolmosť.

Veta 6.10 *Počet usporiadanýcg dvojíc (g,h), kde g je posunutie v grupe $pmg_2(a,b)$ a h je ľubovoľný prvok z $pmg_2(a,b)$, ktorý je na g kolmý, je*

a) $4a^2b^2+4ab^2+4a^2b+8ab$, *ak oba parametre sú párne,*

b) $4a^2b^2+4ab^2+4a^2b+4ab$, *ak a alebo b je nepárne.*

Dôkaz: Z obrázku vidieť, že g môže byť len tvaru $(P^2)^m(P^{-1}Q)^n$, kde $0\leq m<2a$ a $0\leq n<b$. Vezmime h ľubovoľné. Keďže $pmg_2(a,b)=\langle R\rangle .pg_2(b,a)$, potom $h=R^i(P^2)^k(P^{-1}Q)^jP^l$, kde $0\leq i<2, 0\leq k<2a, 0\leq j<b$ a $0\leq l<2$. Ak je h na g kolmé, musí podľa definície platiť $hgh^{-1}=g^{-1}$, čiže:

$$R^i(P^2)^k(P^{-1}Q)^jP^l(P^2)^m(P^{-1}Q)^nP^{-l}(P^{-1}Q)^{-j}(P^2)^{-k}R^i=R^i(P^2)^m(P^{-1}Q)^{j+(-1)^ln-j}R^i$$

tu sme využili, že $(P^2)^k$ patrí v grupe $pg_2(b,a)$ do centra a že $P^l(P^{-1}Q)^nP^{-l}=(P^{-1}Q)^{(-1)^ln}$.

$$=(P^2)^{(-1)^im}(P^{-1}Q)^{(-1)^ln}$$

V poslednej rovnosti sme využili, že $RPR=P^{-1}$ a $RQR=Q^{-1}$, teda $RP^{-1}QR=PQ^{-1}=P^{-1}Q$, čiže prvky R a $P^{-1}Q$ spolu komutujú.

Prvok $(P^2)^{(-1)^im}(P^{-1}Q)^{(-1)^ln}$ sa musí potom rovnať $(P^{-1}Q)^{-n}(P^2)^{-m}=(P^2)^{a-m}(P^{-1}Q)^{b-n}(1)$.

Nech je prvok h taký, že $l=1$, potom platí $(P^2)^{(-1)^im}(P^{-1}Q)^{(-1)^ln}=(P^2)^{a-(-1)^im}(P^{-1}Q)^{b-n}(2)$. Aby sa prvky (1) a (2) rovnali, musia platiť kongruencie $a-(-1)^im\equiv a-m \pmod{2a}$ a $b-n\equiv b-n \pmod b$. Je zrejmé, že druhá z nich platí pre každú z hodnôt n. Nech $i=0$, potom prvá z kongruencií platí pre každé m a potom pre $(i,l)=(0,1)$ je dvojíc (g,h) spolu $2a.b.2a.b=4a^2b^2$. Nech $i=1$, potom druhá kongruencia platí len pre $m=0$ alebo $m=a$, potom bude pre $(i,l)=(1,1)$ dokopy $2.b.2a.b=4ab^2$ dvojíc (g,h).

Nech $l=0$, potom platí $(P^2)^{(-1)^im}(P^{-1}Q)^n=(P^2)^{a-m}(P^{-1}Q)^{b-n}$, potom musia platiť kongruencie $(-1)^im\equiv a-m \pmod{2a}$ a $n\equiv b-n \pmod b$. Nech $i=1$, potom musí platiť $a\equiv 0 \pmod{2a}$, čo platí len pre $a=0$, čo by ale znamenalo, že rád grupy $pmg_2(0,b)$ je 0, potom ale neobsahuje ani neutrálny prvok a grupou nie je. Potom bude mať táto kongruencia riešenie len pre $n=0$, potom $(P^2)^{a-m}(P^{-1}Q)^{b-n}=(P^2)^{-m}=(P^2)^{-m}$, čo má riešenie pre každé m a v tomto prípade pre $(i,l)=(1,0)$ bude dvojíc zodpovedajúcich požiadavkám vety $4a^2b$. Nech $i=0$, potom $2m-a\equiv 0 \pmod{2a}$ a $2n-b\equiv 0 \pmod b$. Nech $n=0$, potom musí platiť $(P^2)^m=(P^2)^{-m}$, teda $m=0$ alebo $m=a$, potom je v tomto prípade $4ab$ dvojíc (g,h). Ak $n\neq 0$, potom musí platiť $m=\frac{a}{2}$ alebo $m=\frac{3a}{2}$ a $n=\frac{b}{2}$. V prípade, že a alebo b je nepárne, potom v tomto prípade nebude existovať ani jedna taká dvojica (g,h), aby spĺňala predpoklady vety. Nech a je párne aj b je párne, potom pre výber m,n máme 2 možnosti a pre výber k,j je $2ab$ možností, čiže pre $(i,l)=(0,0)$ je dvojíc (g,h) $4ab$.

Potom pre a párne a b párne je počet požadovaných dvojíc $4a^2b^2+4ab^2+4a^2b+8ab$, pre a alebo b nepárne $4a^2b^2+4ab^2+4a^2b+4ab$.

čbtd

Teraz už môžeme sformulovať vetu o izomorfizmoch.

Veta 6.11 *Grupy $pmg_2(a,b)$ a $pmg_2(a',b')$ sú izomorfné práve vtedy, ak $(a,b)=(a',b')$.*

Dôkaz: Dokázať túto vetu zprava doľava je triviálne, jedná sa o rovnaké grupy. Nech teda $pmg_2(a,b)$ a $pmg_2(a',b')$ sú izomorfné. Dokážeme, že musí platiť $a=a'$ a $b=b'$.

Nech a aj b sú nepárne, potom musia byť nepárne aj a' a b'. Z rovnosti rádov grúp $pmg_2(a,b)$ a $pmg_2(a',b')$ vieme, že $ab=a'b'(1)$ a dosadením (1) do rovnosti počtu involúcií dostávame $a=a'$.

Nech $a+b \equiv 1 \pmod 2$ a $a'+b' \equiv 1 \pmod 2$, potom z rovnosti počtu involúcií dostávame $a = a'$ a potom $b = b'$. Podobne aj pre a, b, a', b' párne.

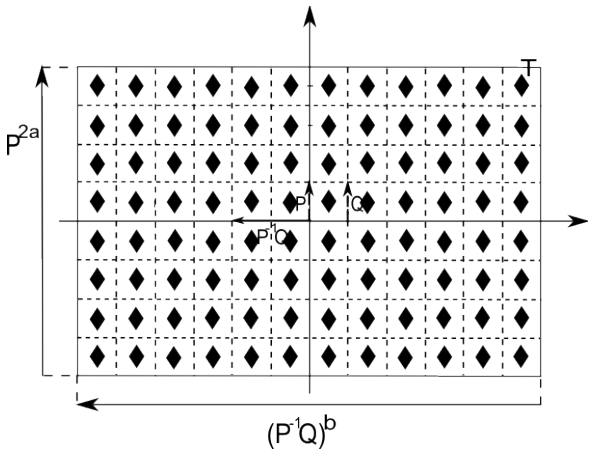
Nech $a + b \equiv 1 \pmod 2$ a a' a b' sú párne. Potom musí platiť $a = a' + 1$. V oboch grupách musí existovať rovnaký počet dvojíc (g, h) vyhovujúcich predchádzajúcej vete. Potom $4a^2b^2 + 4ab^2 + 4a^2b + 4ab = 4a'^2b'^2 + 4a'b'^2 + 4a'^2b' + 8a'b'$. Využijúc rovnosť $ab = a'b'$ a po jednoduchých úpravách $b + a = b' + a' + 1$. Ak využijeme $a = a' + 1$, potom $b = b'$, ale potom $ab = (a' + 1)b' > a'b'$, čo je spor s predpokladom izomorfnosti grúp.
čbtd

6.5 Štrukturálne vlastnosti grupy $pgg_1(a, b)$

Grupa $pgg_1(a, b)$ rovnako ako predchádzajúce dve grupy obsahuje ako svoju podgrupu pg. Jej prezentácia je daná nasledujúcim predpisom:

$$pgg_1(a, b) := \langle P, Q, T | P^2 = Q^2, TPT^{-1} = Q^{-1}, T^2 = P^{2a} = (P^{-1}Q)^b = 1 \rangle . \tag{29}$$

Obrázok (17) nám hovorí, ako si túto grupu môžeme geometricky predstaviť.



Obrázok 17: Grupa $pgg_1(a, b)$

Všimnime si jej podgrupu $H := \langle P, Q | P^2 = Q^2, P^{2a} = (P^{-1}Q)^b = 1 \rangle$. Toto je ale prezentácia grupy $pg_1(b, a)$. Po využití veľkostí grúp dostávame, že H má index 2 a teda je to normálna podgrupa. Grupu $pgg_1(a, b)$ môžeme teda vyjadriť nasledovne $pgg_1(a, b) = \langle T \rangle . pg_1(b, a)$. Na základe predchádzajúcich riadkov vieme sformulovať nasledujúcu vetu.

Veta 6.12 *Každý prvok grupy $pgg_1(a, b)$ danej prezentáciou (29) má jednoznačný tvar*

$$T^i(P^2)^k(P^{-1}Q)^j P^l, \tag{30}$$

kde $0 \le i < 2$, $0 \le k < a$, $0 \le j < b$ a $0 \le l < 2$.

Dôkaz: Keďže sme si na začiatku tejto podkapitoly ukázali, že $pgg_1(a, b) = \langle T \rangle . pg_1(b, a)$, potom každý jej prvok je tvaru $T^i g$, kde $g \in pg_1(b, a)$. Z prezentácie (29) vyplýva, že rád prvku T delí číslo 2, teda, $i \in \{0, 1\}$. Vo vete 5.7 sme si dokázali, že každý prvok grupy $pg_1(b, a)$ je tvaru $(P^2)^k(P^{-1}Q)^j P^l$, kde $0 \le k < a$, $0 \le j < b$ a $0 \le l < 2$. Potom každý prvok grupy $pgg_1(a, b)$ vieme upraviť do tvaru (30), týchto kombinácií je ale $4ab$, čo je veľkosť grupy $pgg_1(a, b)$ a teda prvok je tvarom (30) jednoznače určený.
čbtd

Na určenie izomorfnosti dvoch grúp z rodiny pgg nám poslúžia taktiež počty involúcií.

Veta 6.13 *Počet involúcií v grupe $pgg_1(a,b)$ je*

a) $3+ab$, *ak* a *aj* b *sú párne,*

b) $1+a(b+1)$, *ak* a *je párne a* b *nepárne,*

c) $b+1+ab$, *ak* a *je nepárne a* b *párne a*

d) $b+a(b+1)$, *ak* a *aj* b *sú nepárne.*

Dôkaz: Keďže sme si ukázali, že grupa $pg_1(b,a)$ je podgrupou $pgg_1(a,b)$ indexu 2, bude sa počet involúcií v grupe $pgg_1(a,b)$ rovnať počtu involúcií v $pg_1(b,a)$ plus počet involúcií v množine $T.pg_1(b,a)$.

V prípade a) sú v grupe $pg_1(b,a)$ podľa vety 5.9 3 involúcie, v prípade b) je 1 involúcia, v c) ich je $b+1$ a v prípade d) je počet involúcií b.

Teraz počítajme, koľko je involúcií v množine $T.pg_1(b,a)$. Každý prvok tejto množiny je $T(P^2)^k(P^{-1}Q)^jP^l$, kde $0\le k<a$, $0\le j<b$ a $0\le l<2$. Ukážeme si, pre ktorú trojicu (k,j,l) bude prvok involúciou.

$$\begin{aligned}T(P^2)^k(P^{-1}Q)^jP^lT(P^2)^k(P^{-1}Q)^jP^l &= (TPT)^{2k}T(P^{-1}Q)^jP^l(TPT)^{2k}T(P^{-1}Q)^jP^l\\ &= Q^{-2k}T(P^{-1}Q)^jP^lQ^{-2k}T(P^{-1}Q)^jP^l\end{aligned}$$

Využili sme, že $TP^i=TP^iTT=TPTTPT...TPTT=(TPT)^iT=Q^{-i}T$.

$$\begin{aligned}&= P^{-2k}TP^{-2k}TT(P^{-1}Q)^jP^lT(P^{-1}Q)^jP^l\\ &= T(P^{-1}Q)^jTQ^{-l}(P^{-1}Q)^jP^l\end{aligned}$$

Tu sme využili, že $Q^2=P^2$ a že prvok P^2 patrí do centra grupy pg_1, ďalej sme využili, že $TP^iT=Q^{-i}$, teda $P^iT=TQ^{-i}$.

$$\begin{aligned}&= (QP^{-1})^j(P^{-1}Q)^{(-1)^l(j+l)}\\ &= (P^{-1}Q)^{(-1)^l(j+l)-j}\end{aligned}$$

Znovu využívame, že $TP^iT=Q^{-i}$ a $TQ^jT=P^{-j}$ a ďalej $Q^{-l}(P^{-1}Q)^jP^l=Q^{-l}(PQ^{-1})^jP^l=(P^{-1}Q)^{(-1)^l(j+l)}$.

Z vety 6.12 ďalej vieme, že prvok je určený predpisom (15) jednoznačne. Z toho vyplýva, že ak má platiť $(P^{-1}Q)^{(-1)^l(j+l)-j}=1$, musí $(-1)^l(j+l)-j\equiv 0 \pmod b$. Nech $l=0$, potom má platiť kongruencia $j-j\equiv 0 \pmod b$, to platí pre každé j a k, preto pre $l=0$ bude v množine $T.pg_1(b,a)$ ab involúcií. Nech $l=1$, potom $-2j-1\equiv 0 \pmod b$, čiže $2j\equiv -1 \pmod b$. Vzhľadom na to, že j je minimálne 0 a maximálne $b-1$, môžu nastať len prípady $2j+1=0(1)$ alebo $2j+1=b(2)$. Rovnica (1) nemá riešenie pre žiadne prirodzené j a z (2) dostávame $j=\frac{b-1}{2}$, čo má riešenie len v prípade, že b je nepárne.

Ak to zhrnieme, tak v množine $T.pg_1(b,a)$ je v prípade, že b je párne spolu ab involúcií a v prípade, keď b je nepárne je dokopy $ab+a$ involúcií. Spolu s involúciami z podgrupy $pg_1(b,a)$ je to počet, ktorý sme mali dokázať.

čbtd

Aby sme vedeli dokázať vetu o izomorfizmoch gríp $pgg_1(a,b)$ a $pgg_1(a',b')$, dokážeme si, koľko je prvkov kolmých na posunutie v grupe $pgg_1(a,b)$ a koľko je takých dvojíc.

Veta 6.14 *Počet usporiadaných dvojíc* (g,h), *kde* g *je posunutie v* $pgg_1(a,b)$ *a* h *je ľubovoľný prvok z* $pgg_1(a,b)$ *kolmý na* g *je*

a) $4ab+2ab^2+a^2b^2+2a^2b$, *ak oba parametre sú párne,*

b) $2ab+2ab^2+a^2b^2+a^2b$, *ak* a *je párne a* b *nepárne,*

c) $2ab + ab^2 + a^2b^2 + 2a^2b$, *ak* a *je nepárne a* b *párne a*

d) $ab + ab^2 + a^2b^2 + a^2b$, *ak oba prametre sú nepárne.*

Dôkaz: Každé posuntie v grupe $pgg_1(a,b)$ je tvaru $(P^2)^m(P^{-1}Q)^n$, kde $0 \leq m < a$ a $0 \leq n < b$ (to, že skutočne nemôže nastať iná možnosť posunutia z grupy $pgg_1(a,b)$ vidieť z obrázka (17)). Nech je prvok h tvaru $T^i(P^2)^k(P^{-1}Q)^jP^l$, kde $0 \leq i < 2, 0 \leq k < a, 0 \leq j < b, 0 \leq l < 2$. Aby bol prvok h na g kolmý, potom podľa definície 6.1 musí platiť $hgh^{-1} = g^{-1}$, potom prvok hgh^{-1} je rovný:

$$T^i(P^2)^k(P^{-1}Q)^jP^l(P^2)^m(P^{-1}Q)^nP^{-l}(P^{-1}Q)^{-j}(P^2)^{-k}T^i = T^i(P^2)^m(P^{-1}Q)^jP^l(P^{-1}Q)^nP^{-l}(P^{-1}Q)^{-j}T^i$$

v tomto bode sme využili, že v podgrupe $pg_1(b,a)$ patrí prvok $(P^2)^k$ do centra

$$= T^i(P^2)^m(P^{-1}Q)^{j+(-1)^ln-j}T^i$$

tu sme využili, že $P^l(P^{-1}Q)^nP^{-l} = (P^{-1}Q)^{(-1)^ln}$.

$$= (P^2)^{(-1)^im}(P^{-1}Q)^{(-1)^{l+i}n}$$

V poslednom bode sme využili, že $P^{-1}QT = TQP^{-1} = T(P^{-1}Q)^{-1}$, potom $(P^{-1}Q)^nT^i = T^i(P^{-1}Q)^{(-1)^in}$ a podobne $T^i(P^2)^mT^i = (T^iPT^i)^{2m} = P^{(-1)^i2m}$.

Dostali sme, že ak sú prvky h a posunutie $(P^2)^m(P^{-1}Q)^n$ na seba kolmé, bude platiť $(P^2)^{(-1)^im}(P^{-1}Q)^{(-1)^{l+i}n} = (P^2)^{-m}(P^{-1}Q)^{-n}$. Z vety 6.12 vieme, že každý prvok je daným tvarom vyjadrený jednozančne a teda platí $(-1)^im \equiv -m \pmod a$(1) a $(-1)^{l+i}n \equiv -n \pmod b$(2). Nech $h \in pg_1(b,a)$, potom $i = 0$. Kongruencie sa nám zjednodušia na tvar $m \equiv -m \pmod a$ a $(-1)^ln \equiv -n \pmod b$. Prvá z kongruencí je riešiteľná len pre $m = 0$ alebo $m = \frac{a}{2}$. V druhej pre $l = 0$ musí platiť $n = 0$ alebo $n = \frac{b}{2}$. Pre $l = 0$ máme teda počet dvojíc h, g pre a aj b párne $4ab$, keďže kongruencie platia pre ľubovoľné k a j, pre $a + b \equiv 1 \pmod 2$ je to $2ab$ párov a pre oba parametre nepárne je párov v tomto prípade ab.

Nech $l = 1$, potom podobne ako v predchádzajúcom prípade musí platiť $m = 0$ alebo $m = \frac{a}{2}$ a druhá kongruencia bude vyzerať $-n \equiv -n \pmod b$. Teda, n môžeme vyberať ľubovoľné (a rovnako aj k a j), potom je pre a párne v tomto prípade $2ab^2$ párov a pre a nepárne ab^2.

Nech je teraz $i = 1$, potom $h \in T.pg_1(b,a)$. Kongruencia (1) nadobudne tvar $-m \equiv -m \pmod a$ a (2) bude $-(-1)^ln \equiv -n \pmod b$. Podobnými úvahami ako v predchádzajúcom prípade by sme dospeli ku záveru, že pre $l = 0$ bude vyhovujúcich párov a^2b^2 a pre $l = 1$ bude pre b párne $2a^2b$ a pre b nepárne a^2b párov.

čbtd

Teraz už môžeme sformulovať vetu o izomorfizmoch.

Veta 6.15 *Grupy* $pgg_1(a,b)$ *a* $pgg_1(a',b')$ *sú izomorfné práve vtedy, keď* $(a,b) = (a',b')$ *alebo* $(a,b) = (b',a')$.

Dôkaz:

(„⇐")

Ak $(a,b) = (a',b')$, potom sa jedná o totožné grupy.

Nech $(a,b) = (b',a')$, potom vezmime zobrazenie:

$$\varphi : P \longmapsto P'^{-1}T'$$
$$\varphi : T \longmapsto P'^{-1}T'P'$$
$$\varphi : Q \longmapsto P'^{-1}T'P'^2.$$

Aby sme overili, že je to homomorfizmus, musíme dokázať rovnosť $\varphi(T)\varphi(P)\varphi(T) = \varphi(Q^{-1}) = \varphi(TPT)$ a že neutrálne prvky sa zobrazia na neutrálne.

$$\varphi(T)\varphi(P)\varphi(T) = P'^{-1}T'\underbrace{P'P'^{-1}}_{=1}T'P'^{-1}T'P' = P'^{-1}\underbrace{T'T'}_{=1}P'^{-1}T'P'$$
$$= P'^{-2}T'P' = (P'^{-1}T'P'^{2})^{-1} = \varphi(Q)^{-1} = \varphi(Q^{-1}) = \varphi(TPT).$$

$$\varphi(1) = \varphi(T^2) = \varphi(T)^2 = P'^{-1}T'P'P'^{-1}T'P' = 1$$
$$= \varphi(P^2Q^{-2}) = \varphi(P)^2\varphi(Q)^{-2} = P'^{-1}T'P'^{-1}T'P'^{-2}T'P'P'^{-2}T'P' = P'^{-1}Q'P'^{-2}Q'P' =$$
$$= P'^{-1}Q'Q'^{-2}Q'P' = 1$$
$$= \varphi(P^{2a}) = \varphi(P)^{2a} = \underbrace{P'^{-1}T'P'^{-1}T'...}_{2a\text{- krát}} = (P'^{-1}Q)^a = (P'^{-1}Q)^{b'} = 1$$
$$= \varphi((P^{-1}Q)^b) = (\varphi(P)^{-1}\varphi(Q))^b = (T'P'P'^{-1}T'P'^{2})^{a'} = P'^{2a'} = 1.$$

Teraz dokážeme, že je to surjektívne zobrazenie. Vzľadom na to, že do grupy $Im(\varphi)$ patria prvky $T'P'P'^{-1}T'P' = P'$, $P'P'^{-1}T' = T'$ a potom aj $T'P'^{-1}T' = Q'$, potom $Im(\varphi)$ je celá grupa $pgg_1(a', b')$ a zobrazenie φ je izomorfizmus.
(„⇒")
Teraz ukážeme, že ak sú $pgg_1(a, b)$ a $pgg_1(a', b')$ izomorfné, potom $(a, b) = (a', b')$ alebo $(a, b) = (b', a')$. Dokážeme to sporom. Nech existujú také dvojice parametrov $(a, b) \neq (a', b')$ a $(a, b) \neq (b', a')$, pre ktoré budú $pgg_1(a, b)$ a $pgg_1(a', b')$ izomorfné.

I. Nech a aj b sú nepárne, potom je počet involúcií v grupe $pgg_1(a, b)$ rovný číslu $b+ab+a$. Keďže využitím rovnosti rádov grúp dostávame rovnosť $ab = a'b'(1)$, musia byť aj a' a b' nepárne, teda v grupe $pgg_1(a', b')$ je $b' + a'b' + b'$ involúcií. Počty involúcií sa musia rovnať, dostávame rovnicu $a + b = a' + b'$. Táto rovnica bola v tomto texte už viackrát riešená a musí platiť $(a, b) = (a', b')$ alebo $(a, b) = (b', a')$.

II. Nech a je párne a b nepárne. V grupe $pgg_1(a, b)$ je potom $1 + ab + a$ involúcií. Keďže $2|ab$, potom musí byť aspoň jeden z parametrov a', b' párny.

   a) Nech a' je párne a b' nepárne, potom je v grupe $pgg_1(a', b')$ $1 + a'b' + a'$ involúcií. Po využití rovnosti (1) a rovnosti počtu involúcií dostávame $a = a'$ a teda aj $b = b'$.

   b) Nech a' je nepárne a b' je párne. V grupe $pgg_1(a', b')$ je potom $a'b' + b' + 1$ involúcií. Z čoho $a = b'$ a $b = a'$.

   c) Nech sú párne aj a', aj b'. Počet involúcií v grupe $pgg_1(a', b')$ je $3 + a'b'$. Potom musí platiť rovnosť $2 = a$. Ale keďže b je nepárne, potom štvorka nedelí súčin ab, ale $a'b'$ delí, čo je spor.

III. Nech je a nepárne a b párne. V tomto prípade je v grupe $pgg_1(a, b)$ dokopy $ab+b+1$ involúcií.

   d) Nech je a' párne a b' nepárne. Potom sa jedná o obrátený izomorfimus prípadu $II.b$).

   e) Nech a' je nepárne a b' párne. Potom využitím rovnosti počtu involúcií a (1) platí $b = b'$.

   f) Nech sú oba parametre grupy $pgg_1(a', b')$ párne. Dostávame rovnosť $b = 2$. Analogicky ako v prípade $II.c$) dokážeme, že takýto prípad nastať nemôže.

IV. Nech sú a aj b párne. V grupe $pgg_1(a, b)$ bude potom $3 + ab$ involúcií.

   g) Nech $a' + b' \equiv 1 \pmod 2$, potom sme v prípadoch $II.c$) a $III.f$) dokázali, že takéto grupy izomorfné byť nemôžu.

h) Nech a' aj b' sú párne. V oboch grupách $(pgg_1(a,b)$ a $pgg_1(a',b'))$ je rovnaký počet involúcií. V grupe $pgg_1(a,b)$ bude podľa vety 7.13 párov vyhovujúcich vete $4ab + 2ab^2 + a^2b^2 + 2ab^2$, rovnaký počet musí byť aj v grupe $pgg_1(a',b')$. Využijúc rovnosť $ab = a'b'$ a po jednoduchých úpravách, dostávame rovnicu tvaru $a + b = a' + b'$, ktorú sme v tomto texte už viackrát počítali a jej výsledok je $a = a'$ alebo $b = b'$.

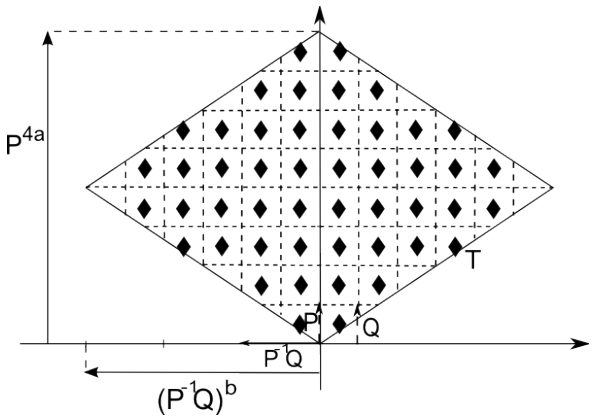
čbtd

6.6 Štrukturálne vlastnosti grupy $pgg_2(a,b)$

Aj grupa $pgg_2(a,b)$ bude vychádzať z grupy pg. Určená je prezentáciou:

$$pgg_2(a,b) := \langle P, Q, T | P^2 = Q^2, TPT^{-1} = Q^{-1}, T^2 = P^{2a}(P^{-1}Q)^b = P^{4a} = 1 \rangle . \tag{31}$$

Grupa $pgg_2(a,b)$ je znázornená na obrázku (18). Vidíme na ňom, že z geometrického hľadiska sa v tejto grupe nachádzajú posunutia, rotácie o π radiánov a vertikálne i horizontálne posunuté zrkadlenia.



Obrázok 18: Grupa $pgg_2(a,b)$

V prípade grupy $pgg_2(a,b)$ budeme postupovať inak ako v predchádzajúcich prípadoch. Najprv si dokážeme niekoľko všeobecných viet o podgrupách.

Veta 6.16 *Nech sú grupy G a G' izomorfné a nech φ je izomorfizmom medzi týmito dvoma grupami. Potom platí:*

a) $N \triangleleft G$ práve vtedy, keď $\varphi(N) \triangleleft G'$,

b) H je cyklickou podgrupou grupy G práve vtedy, keď $\varphi(H)$ je cyklickou podgrupou grupy G',

c) prvky g a h patriace do G spolu komutujú práve vtedy, keď spolu komutujú prvky $\varphi(g)$ a $\varphi(h)$ v grupe G'.

Dôkaz:

a) Nech je $N \triangleleft G$, potom ukážeme, že je aj $\varphi(N) \triangleleft G'$. Keďže je φ izomorfizmom, potom platí $\varphi(N) = \varphi(gNg^{-1}) = \varphi(g)\varphi(N)\varphi(g)^{-1}$, kde g je ľubovoľný prvok grupy G. Zobrazenie φ je surjektívne, potom platí $\varphi(N) = h\varphi(N)h^{-1}$, kde h je ľubovoľný prvok z G'. Druhým smerom sa to dokáže analogicky, ako izomorfizmus vezmeme φ^{-1}.

b) Nech je podgrupa H cyklickou podgrupou grupy G generovanou prvkom h, potom keďže je φ izomorfizmom, potom platí $\varphi(h^n) = \varphi(h)^n$, čo znamená, že obraz podgrupy H je znovu cyklický, generovaný prvkom $\varphi(h)$. Opäť ako v predošlom prípade, na dôkaz opačnej implikácie použijeme zobrazenie φ^{-1} a postupujeme analogicky.

c) Nech g a h komutujú, potom platí $\varphi(g)\varphi(h) = \varphi(gh) = \varphi(hg) = \varphi(h)\varphi(g)$, teda komutujú aj ich obrazy. Nech spolu komutujú prvky $\varphi(g)$ a $\varphi(h)$ patriace do grupy G', potom platí $\varphi(gh) = \varphi(g)\varphi(h) = \varphi(h)\varphi(g) = \varphi(hg)$. Keďže je φ izomorfizmom, potom je to injektívne zobrazenie a platí $gh = hg$, teda aj vzory komutujúcich prvkov spolu komutujú.

čbtd

Ak uplatníme prvé dve z predošlých tvrdení, dostávame, že N je cyklická normálna podgrupa grupy G práve vtedy, keď $\varphi(N)$ je cyklická normálna podgrupa grupy G'.

Najprv musíme nájsť rád prvku P grupy $pgg_2(a,b)$.

Veta 6.17 *Rád prvku P v grupe $pgg_2(a,b)$ je $4a$.*

Dôkaz: Z obrázka (18) vidíme, že pre menšiu mocninu ako $4a$ nedostaneme identické zobrazenie, z prezentácie (31) ale vidíme, že nám stačí mocnina $4a$.
čbtd

Dôsledok 6.2 *I. Rád prvku $P^{-1}Q$ v grupe $pgg_2(a,b)$ je $2b$.*

II. Rád prvku PT v grupe $pgg_2(a,b)$ je $4b$.

Taktiež budeme potrebovať poznať štruktúru podgrupy translácií grupy $pgg_2(a,b)$.

Veta 6.18 *Podgrupa translácií grupy $pgg_2(a,b)$ je rádu $2ab$ a v prípade, že $gcd(a,b) = 1$, bude táto podgrupa cyklická a normálna.*

Dôkaz: Z obrázka (18) vidíme, že skutočne sa v grupe $pgg_2(a,b)$ nachádza práve $2ab$ posunutí. Podgrupa translácií je abelovská a podľa vety 4.1 je izomorfná súčinu cyklických podgrúp. Musíme nájsť jej exponent. Tým je číslo:

$$lcm(Order(P^2), Order(P^{-1}Q)) = lcm(2a, 2b) = 2lcm(a,b) = 2\frac{ab}{gcd(a,b)}.$$

Vidíme, že ak $gcd(a,b) = 1$, bude exponentom číslo $2ab$ a keďže je rád podgrupy translácií rovný tomuto číslu, bude daná grupa cyklická.

Ukážeme, že potom je to normálna podgrupa grupy $pgg_2(a,b)$. Konjugáciou posunutia posunutím, rotáciou o π radiánov a posunutým zrkadlením dostaneme ale opäť posunutie, teda $gHg^{-1} = H$, čo znamená, že podgrupa translácií je normálna podgrupa.
čbtd

Pri tejto grupe budeme pracovať najmä s cyklickými podgrupami grupy $pgg_2(a,b)$. Taktiež s prvkami, ktoré komutujú s posunutými zrkadleniami.

Veta 6.19 *V grupe $pgg_2(a,b)$ platí:*

a) ak prvok g z grupy $pgg_2(a,b)$ komutuje s prvkom P, potom patrí do $\langle P\rangle$,

b) ak $b \neq 1$, potom podgrupa $\langle P\rangle$ nie je normálna,

c) ak prvok g z grupy $pgg_2(a,b)$ komutuje s prvokm PT, potom patrí do $\langle PT\rangle$,

d) ak $a \neq 1$, potom podgrupa $\langle PT\rangle$ nie je normálna.

Dôkaz: Ukážeme prípad a), potom c) sa dokáže analogicky. Nech g komutuje s posunutým zrkadlením P.

Z vety 2.2, ak prvok h fixuje množinu A, potom prvok ghg^{-1} fixuje množinu gA. V našom prípade je prvkom h posunuté zrkadlenie P, ktoré fixuje os reflexie. Ak nejaký prvok g komutuje so zobrazením P, potom bude zobrazenie gPg^{-1} fixovať os reflexie P.

Nech je prvok g posunutím, potom zrejme každé z posunutí je tvaru $(P^2)^k(P^{-1}Q)^j$. Konjugácia posunutého zrkadlenia P posunutím $(P^2)^k(P^{-1}Q)^j$ bude zachovávať priamku $(P^2)^k(P^{-1}Q)^j.R$, kde R je os reflexie prvku P. Potom je zrejmé, že $(P^{-1}Q)^j$ bude v grupe $pgg_2(a,b)$ neutrálnym prvkom alebo mocninou posunutia P^2. Teda $j=0$ alebo $j=b$ a pre každé l bude $(P^2)^l \in \langle P\rangle$.

Nech je prvok g rotáciou o π radiánov. Konjugáciou takouto rotáciou ale dostaneme posunuté zrkadlenie, ktoré posúva opačným smerom ako P. Aby sa tieto posunutia rovnali, musí platiť $P^2=1$, čo je ale spor s vetou 6.17.

Nech je prvkom g rovnobežné posunuté zrkadlenie s P, potom prvok gPg^{-1} fixuje priamku, ktorá je od R posunutá o $(P^{-1}g)^{-2}$, potom ale toto posunutie musí byť jednotkou. Prvok $(P^{-1}g)^{-2}$ je ale zrejme mocninoou $P^{-1}Q$, potom $P^{-1}g=(P^{-1}Q)^b=P^{2a}$ alebo $P^{-1}g=1$, čo v oboch prípadoch znamená, že g je od P vzdialené len o mocninu P.

Nech je prvkom g kolmé posunuté zrkadlenie na P. Konjugácia posunutého zrkadlenia P prvkom g ale posúva o rovnakú veľkosť ale opačným smerom ako P, keďže predpokladáme, že $gPg^{-1}=P$, potom sa posunutia musia rovnať, potom platí $P^2=1$, čo je spor s rádom prvku P.

Ukážeme bod b) a d) sa dokáže analogicky. Konjugujme posunuté zrkadlenie P posunutím $(P^{-1}Q)^{-1}=Q^{-1}P$, dostávame, že takéto zobrazenie fixuje množinu R len v prípade, že $(P^{-1}Q)^{-1}$ je mocninou prvku P. To nastáva vtedy, keď $b=1$.
čbtd

Pomocou zobrazení dokážeme aj nasledujúcu vetu.

Veta 6.20 *Nech sú grupy $pgg_2(a,b)$ a $pgg_2(a',b')$ izomorfné, potom obrazom posunutého zrkadlenia P musí byť znovu posunuté zrkadlenie. Podobne obrazom posunutého zrkadlenia PT musí byť tiež posunuté zrkadlenie. Pričom, ak $b\neq 1$, potom obrazy P a PT majú kolmé osi reflexie.*

Dôkaz: Ukážeme, že obrazom posunutého zrkadlenia P musí byť posunuté zrkadlenie. Keďže rád rotácie je 2, potom zrejme žiadna rotácia o π radiánov nebude obrazom posunutého zrkadlenia, ktoré má rád minimálne 4. Nech sa teda zobrazí do posunutia. S posunutým zrkadlením P komutuje ale práve $4a$ prvkov a s posunutím minimálne $2a'b'=2ab$, čo pre $b>2$ bude viac ako $4a$.

Nech je teda $b=2$. Potom podgrupa translácií v grupe $pgg_2(a',b')$ má veľkosť $2a'b'=4a$. Keďže je P rádu $4a$, musí existovať posunutie, ktoré je rádu $4a$, potom je ale podgrupa translácií cyklická a podľa vety 6.18 je aj normálna. Podgrupa $\langle P\rangle$ podľa vety 6.19 cyklická nie je, čo je spor s vetou 6.16, podľa ktorej ak je obrazom podgrupy H normálna podgrupa, musí byť aj H normálna. Potom sa musí posunuté zrkadlenie P zobraziť na posunuté zrkadlenie v grupe $pgg_2(a',b')$.

Nech je $b=1$, potom zrejme má každé posunutie v grupe $pgg_2(a',b')$ rád nanajvýš $2a'b'=2ab=2a<4a$, čo je spor s predpokladom, že P sa zobrazí na posunutie.

Analogicky by sme ukázali, že aj obrazom posunutého zrkadlenia PT je posunuté zrkadlenie v grupe $pgg_2(a',b')$.

Teraz ukážeme, že obrazy posunutých zrkadlení P a PT sú kolmé. Dokážeme to sporom. Z vety 6.16 ale vieme, že obrazy prvkov g a h spolu komutujú práve vtedy, keď komutujú aj samotné prvky g a h. V prípade, že sa P a PT zobrazia na rovnobežné posunuté zrkadlenia, bude platiť $\varphi(PT)^2\varphi(P)=\varphi(P)\varphi(PT)^2$, teda prvok $PTPT=P^{-1}Q$ musí podľa vety 6.19 patriť do podgrupy $\langle P\rangle$, čo je možné ale len v prípade, že $b=1$.
čbtd

Vďaka predchádzajúcim vetám môžeme sformulovať nasledujúcu vetu.

Veta 6.21 *Grupy $pgg_2(a,b)$ a $pgg_2(a',b')$ sú izomorfné práve vtedy, keď $(a,b)=(a',b')$ alebo $(a,b)=(b',a')$.*

Dôkaz:
(„$\Leftarrow$")
Nech $(a,b)=(a',b')$, to že sú grupy $pgg_2(a,b)$ a $pgg_2(a',b')$ izomorfné je zrejmé, keďže sa jedná o rovnaké grupy.

Nech $(a,b)=(b',a')$, potom vezmime predpis:

$$\varphi : P \longmapsto P'^{-1}T'$$
$$\varphi : T \longmapsto P'^{-1}T'P'$$
$$\varphi : Q \longmapsto P'^{-1}T'P'^{2}.$$

Najprv musíme ukázať, že sa jedná o zobrazenie. Znamená to ukázať, že platí rovnosť $\varphi(T)\varphi(P)\varphi(T)\varphi(Q) = \varphi(P)^2\varphi(Q)^{-2} = \varphi(T)^2 = \varphi(P)^{2a}(\varphi(P)^{-1}\varphi(Q))^b = \varphi(P)^{4a} = 1(1)$.

$$\begin{aligned}
1 &= \varphi(TPTQ) = \varphi(T)\varphi(P)\varphi(T)\varphi(Q) = P'^{-1}T'P'P'^{-1}T'P'^{-1}T'P'P'^{-1}T'P'^{2} = 1\\
&= \varphi(P^2Q^{-2}) = \varphi(P)^2\varphi(Q)^{-2} = P'^{-1}T'P'^{-1}T'P'^{-2}T'P'P'^{-2}T'P' = P'^{-1}Q'\underbrace{P'^{-2}}_{=Q'^{-2}}Q'P' = 1\\
&= \varphi(T^2) = \varphi(T)^2 = P'^{-1}T'P'P'^{-1}T'P' = 1\\
&= \varphi(P^{2a}(P^{-1}Q)^b) = \varphi(P)^{2a}(\varphi(P)^{-1}\varphi(Q))^b = (P'^{-1}T')^{2a}(T'P'P'^{-1}T'P'^{2})^b =\\
&\quad = (P'^{-1}T'P'^{-1}T')^aP'^{2b} = (P'^{-1}Q')^{b'}P'^{2a'} = 1\\
&= \varphi(P^{4a}) = \varphi(P)^{4a} = (P'^{-1}T'P'^{-1}T')^{2a} = (P'^{-1}Q')^{2a} = 1.
\end{aligned}$$

Keďže sme rovnosti (1) dokázali, bude φ homomorfizmom. Ukážeme, že sa jedná o izomorfizmus. Do grupy $Im(\varphi)$ patrí prvok $P'^{-1}T'$ a tiež $P'^{-1}T'P'$, potom tam patrí aj ich súčin, teda prvok P'^{-1} a keďže je to grupa, potom aj jeho inverz, teda P'. Potom tam patrí ale aj prvok T' a teda aj $T'P'T' = Q'^{-1}$. Keďže do podgrupy $Im(\varphi)$ patria všetky generujúce prvky grupy $pgg_2(a',b')$, bude zobrazenie surjektívne a z rovnosti veľkosti grúp (keďže $ab = a'b'$) vyplýva, že sa jedná o bijektívne zobrazenie, čiže izomorfizmus.
(„⇒")
Nech sú grupy $pgg_2(a,b)$ a $pgg_2(a',b')$ izomorfné. Dokážeme, že musí platiť $(a,b) = (a',b')$ alebo $(a,b) = (b',a')$. Podľa vety 6.20 sa musí posunuté zrkadlenie zobraziť do posunutého zrkadlenia. Potom v grupe $pgg_2(a,b)$ existuje posunuté zrkadlenie rádu $4a$ a $4b$. Teda, ak $a|a'$, potom $b|b'$ alebo ak $a|b'$, potom $b|a'$, čo vyplýva z toho, že pre $b \neq 1$ obrazy posunutých zrkadlení P a PT musia mať kolmé osi reflexie. Keďže $ab = a'b'$, potom $(a,b) = (a',b')$ alebo $(a,b) = (b',a')$. Nech $b = 1$, potom $a = a'b'$ a keďže $a|a'$ alebo $a|b'$, potom $a = a'$ alebo $a = b'$ a zároveň $b' = 1$ alebo $a' = 1$.
čbtd

Záver

Táto práca mala za úlohu zistiť, kedy sú niektoré z kvocientov tapetových grúp izomorfné. Zaoberali sme sa grupami $p1(a,b;c), p2(a,b;c), pm_1(a,b), pm_2(b,c), pg_1(a,b), pg_2(a,b), cm_1(a,b), cm_2(a,b)$, $pmm_1(a,b), pmm_2(a,b), pmg_1(a,b), pmg_2(a,b), pgg_1(a,b)$ a $pgg_2(a,b)$. Samozrejme, dalo by sa pokračovať a nájsť izomorfizmy všetkých z kvocientov, no nám sa to pre nedostatok času nepodarilo. Tak napríklad sa domnievame, že grupy $p4(a,b)$ a $p4(a',b')$ budú izomorfné jedine vtedy, keď sa budú ich parametre rovnať alebo bude platiť $(a,b) = (b',a')$.

Podobne by sme mohli ísť ďalej a skúmať izomorfizmy medzi jednotlivými kvocientami. Niektoré sme pri našej práci našli, napríklad:

Veta 6.22 *Grupy $p1(a,b;c)$ a $p2(a',b';c')$ sú izomorfné práve vtedy, keď $ab = 2$ a $a' = b' = 1$ alebo $a = b = 2$ a $c = 2k$ a $a'b' = 2$.*

Dôkaz: Ak $ab = 2$, potom grupa $p1(a,b;c)$ je izomorfná grupe Z_2. Grupa $p2(1,1;c')$ je izomorfná grupe Z_2, teda obe sú izomorfné rovnakej grupe.

Ak $gcd(a,b,c) = 2$ a $a = b = 2$, potom je grupa $p1(a,b;c) \cong Z_2 \times Z_2$. Grupa $p2(a',b';c')$ je daná ako $\langle T \rangle .p1(a',b';c')$. V tomto prípade ale $p1(a',b';c') \cong Z_2$, potom $p2(a',b';c') \cong Z_2 \times Z_2$.

Nech sú grupy $p1(a,b;c)$ a $p2(a',b';c')$ izomorfné. V stati o štrukturálnych vlastnostiach grupy $p2(a',b';c')$ sme si ukázali, že každý prvok patriaci do množiny $T.p1(a',b';c')$ je rádu 2, takýchto prvkov je $a'b'$. V grupe $p1(a,b;c)$ sú maximálne 3 involúcie (2 involúcie grupa $p1(a,b;c)$ nikdy nemá). V $p2(a',b';c')$ sa nachádza na základe predchádzajúceho minimálne $a'b'$ involúcií. Potom $a' = b' = 1$ alebo $a'b' + 1 = 3$ alebo $a'b' = 3$. Prípad, keď $a'b' = 1$ a $a'b' = 2$ sme si ukázali v predošlých riadkoch. Nech $a'b' = 3$. Potom ale $ab = 6$, čo sa nedá nikdy rozložiť na súčin dvoch párnych čísel a v tomto prípade má grupa $p1(a,b;c)$ len 1 involúciu, potom v takomto prípade nie sú $p1(a,b;c)$ a $p2(a',b';c')$ nikdy izomorfné.
čbtd

Existujú taktiež ďalšie grupy, ktoré sú pre niektoré parametre abelovské. Potom sú podľa vety 4.1 izomorfné súčinu cyklických grúp. To, či sú potom izomorfné s grupou $p1(a',b';c')$ sa už takmer vo všetkých prípadoch dokáže pomocou vety 4.8.

Veta 6.23 *Grupy $p1(a,b;c)$ a $pm_1(a',b')$ sí izomorfné jedine vtedy, keď $ab = 2a'b'$*

- *$a' = 1$ a zároveň $gcd(a,b,c) = gcd(2,b')$ alebo*
- *$a' = 2$ a zároveň $gcd(a,b,c) = 2$ a $gcd(2,b') = 1$.*

Dôkaz: V prípade, že $b' \geq 3$, potom grupa $pm_1(a,b)$ obsahuje ako svoju podgrupu $D_{2b'}$, ktorá má triviálne centrum a teda grupa $pm_1(a,b)$ nebude abelovská.

Nech $a' = 1$, potom je grupa $pm_1(a',b') \cong Z_{b'} \times Z_2$. Grupa $p1(a,b;c)$ je izomorfná grupe $Z_{gcd(a,b,c)} \times Z_{\frac{ab}{gcd(a,b,c)}}$. Grupy $Z_{b'} \times Z_2$ a $Z_{gcd(a,b,c)} \times Z_{\frac{ab}{gcd(a,b,c)}}$ sú podľa vety 4.8 izomorfné práve vtedy, keď $2b' = 2a'b' = ab$. Ďalej musí platiť $gcd(2,b') = gcd(gcd(a,b,c), \frac{ab}{gcd(a,b,c)}) = gcd(a,b,c)$.

Nech $a' = 2$, potom $pm_1(2,b') \cong Z_{b'} \times Z_2 \times Z_2$. V prípade, že b' je párne, by táto grupa potrebovala až tri generátory, no $p1(a,b;c)$ má len 2, potom musí platiť $gcd(b',2) = 1$ a $pm_1(2,b') \cong Z_{2b'} \times Z_2$. Znovu použijeme vetu 4.8, podľa ktorej ak sú $Z_{2b'} \times Z_2$ a $Z_{gcd(a,b,c)} \times Z_{\frac{ab}{gcd(a,b,c)}}$ izomorfné, musí platiť $4b' = 2a'b' = ab$ a $gcd(2b',2) = 2 = gcd(a,b;c)$.
čbtd

Podobne by sme našli izomorfizmus aj medzi grupami $pm_2(1,b)$ a $p1(a',b';c')$, ktoré sú izomorfné práve vtedy, keď $4b = a'b'$ a $gcd(a',b',c') = 2$.

Ďalším príkladom grupy izomorfnej $p1(a,b;c)$ je $pg_1(1,b')$, resp. $pg_1(2,b')$.

Veta 6.24 *1. Grupa $pg_1(1,b)$ je izomorfná grupe $p1(a',b';c')$ práve vtedy, ak $gcd(a',b',c') = 1$ a zároveň $2b = a'b'$.*

2. *Grupa* $pg_1(2,b)$ *je izomorfná grupe* $p1(a',b';c')$ *práve vtedy, ak* $gcd(a',b',c') = 2$ *a zároveň* $4b = a'b'$.

Dôkaz: Dokážme bod 1.). Vo vete o centre grupy $pg_1(1,b)$ sme dospeli k výsledku, že $P = Q$, a teda je grupa cyklická. Jej veľkosť je $2b$ a generátorom je prvok P. Ak $gcd(a',b',c') = 1$, potom je grupa $p1(a',b';c')$ podľa vety 4.6 izomorfná cyklickej grupe s rádom $a'b'$. Dve cyklické grupy sú izomorfné práve vtedy, keď sa ich rády rovnajú, potom $2b = a'b'$. Dokážme to opačným smerom, potom sú ale obe grupy $pg_1(1,b)$ a $p1(a',b';c')$ izomorfné rovnakej grupe.

Dokážme bod 2.). Vo vete o štruktúre prvku v grupe $pg_1(a,b)$ sme dospeli k výsledku, že každý prvok je tvaru $(P^2)^k(P^{-1}Q)^jP^l$, kde $0 \leq k < b$, $0 \leq j < a$, $0 \leq l < 2$, keďže je grupa $pg_1(2,b)$ abelovská (z vety 5.8), vieme transformovať tento tvar na nasledujúci: $P^{2k-j+l}Q^j$. Z prezentácie (14) vieme, že $P^2 = Q^2$, potom keď využijeme, že existujú také prirodzené čísla m a n, že $j = 2m + n$, kde $0 \leq n < 2$, dostaneme:

$$P^{2k-j+l}Q^j = P^{2k-j+l}Q^{2m+n} = P^{2k-j+l}(Q^2)^mQ^n = P^{2k-j+l}P^{2n}Q^n = P^{2k-j+l+2m}Q^n.$$

Kde ak označíme číslo $2k + l + 2m - j = i$, potom dostávame, že v grupe $pg_1(2,b)$ sú všetky prvky tvaru P^iQ^n, kde $i \in \{0,1,...,2b-1\}$ a $n \in \{0,1\}$. Keďže je to abelovská grupa a $P \neq Q$ (to by bol spor s predpokladom, že rád prvku $P^{-1}Q$ je 2), potom je izomorfná grupe $Z_{2b} \times Z_2$. Rovnako je ale tejto grupe izomorfná grupa $p1(a',b';c')$, pre ktorú platí $gcd(a',b',c') = 2$ a $\frac{a'b'}{gcd(a',b',c')} = \frac{4b}{2} = 2b$.
čbtd

Keďže sme si vo vete 5.12 dokázali, že pre $a = 1$ je grupa $pg_2(a,b)$ abelovská, potom bude existovať grupa $p1(a',b';c')$, ktorá je s $pg_2(1,b)$ izomorfná.

Veta 6.25 *Grupa* $pg_2(1,b)$ *je izomorfná grupe* $p1(a',b',c')$ *práve vtedy, keď* $gcd(a',b',c') = 1$ *a súčasne* $4b = a'b'$.

Dôkaz: Z prezentácie (16) vieme, že $P^{-1}Q = P^{2b}$, potom $Q = P^{2b+1}$, čiže grupa $pg_2(1,b) \cong Z_{4b}$. Aby bola grupa $p1(a',b';c')$ cyklická, musí platiť $gcd(a',b',c') = 1$. Ak $4b = a'b'$, potom sú izomorfné rovnakej grupe.
čbtd

Podobnými úvahami vieme sformulovať aj nasledujúcu vetu pre $cm_1(a,b)$.

Veta 6.26 *Grupa* $cm_1(a,b)$ *je s grupou* $p1(a',b';c')$ *izomorfná práve vtedy, keď* $|a-b| = 1$, $2(a+b) = a'b'$ *a* $gcd(a',b',c') = 1$.

Dôkaz: Vo vete 5.15 sme si ukázali, že $cm_1(a,b)$ je abelovská jedine pre $|a-b| = 1$, potom každý jej prvok má tvar S^kR^i, kde $0 \leq k < a+b$ a $0 \leq i < 2$. Keďže $|a-b| = 1$, potom $a + b \equiv 1 \pmod 2$ a prvok SR bude rádu $2(a+b)$, čo je veľkosť celej grupy $cm_1(a,b)$. Potom je grupa $cm_1(a,b)$ cyklická $Z_{2(a+b)}$. Aby bola aj grupa $p1(a',b';c')$ cyklická rádu $2(a+b)$, musí platiť $a'b' = 2(a+b)$ a $gcd(a',b',c') = 1$.

Naopak, nech $gcd(a',b',c') = 1$, $2(a+b) = a'b'$ a $|a-b| = 1$, potom sú grupy $cm_1(a,b)$ a $p1(a',b';c')$ izomorfné rovnakej grupe.
čbtd

Nielen cm_1 je pre vhodné parametre izomorfná grupe $p1$, podobne ukážeme aj vetu pre $cm_2(a,b)$.

Veta 6.27 *Grupa* $cm_2(a,b)$ *je izomorfná grupe* $p1(a',b';c')$ *práve vtedy, keď* $a = 1$, $a'b' = 4b$ *a* $gcd(a',b',c') = 2$.

Dôkaz: Vo vete 5.18 sme si dokázali, že grupa $cm_2(1,b)$ je abelovská, ktorej prvky sú S^kR^i, kde $0 \leq k < 2b$ a $0 \leq i < 2$. Keďže $gcd(2b,2) = 2$, potom je grupa $cm_2(1,b)$ izomorfná grupe $Z_{2b} \times Z_2$. Aby bola rovnakej grupe izomorfná aj $p1(a',b';c')$, musí platiť podľa vety 4.8 $a'b' = 4b$ a $gcd(2b,2) = 2 = gcd(a',b',c')$.
čbtd

V ďalších grupách sme si už centrá neodvodzovali, keďže väčšinou boli len triviálne. Ale vzhľadom na to, že sme si odvodili štruktúru grupy $pmm_1(a,b)$, vieme sformulovať požiadavky, aby $pmm_1(a,b)$ bola komutatívna a izomorfná nejakej $p1(a',b';c')$.

Veta 6.28 *Grupa $pmm_1(a,b)$ je izomorfná grupe $p1(a',b';c')$ práve vtedy, keď $a=b=1$ a $(a',b',c')=(2,2,2k)$, kde k je ľubovoľné.*

Dôkaz: Vo vete 6.1 sme si dokázali, že grupa $pmm_1(a,b) \cong D_{2a} \times D_{2b}$. Pre $a \geq 3$ alebo $b \geq 3$ bude aspoň jedna z podgrúp D_{2a} alebo D_{2b} nekomutatívna. Teda, $a \leq 2$ a zároveň $b \leq 2$. Nech $a=2$ alebo $b=2$, potom je grupa $pmm_1(a,b)$ izomorfná $Z_2 \times Z_2 \times Z_2 \times Z_{\frac{ab}{2}}$. Z dôkazu lemy 4.2 ale vieme, že takúto grupu generujú aspoň tri prvky, ale každú grupu $p1(a',b';c')$ generujú maximálne dva prvky. Z toho nám plynie $a=b=1$, potom je grupa $pmm_1(1,1) \cong Z_2 \times Z_2$. Aby bola $p1(a',b';c')$ izomorfná $Z_2 \times Z_2$, potom musí platiť $a'b'=4$ a $gcd(a',b';c')=2$.
čbtd

Ďalším príkladom izomorfizmov medzi jednotlivými kvocientami tapetových grúp je vzťah medzi $pg_1(a',b')$ a $pg_2(a,b)$.

Veta 6.29 *Ak $(a',b')=(a,2b)$, kde a' je nepárne, potom grupy $pg_1(a',b')$ a $pg_2(a,b)$ sú izomorfné.*

Dôkaz: Nech teda a' je nepárne a $(a',b')=(a,2b)$. Dokážeme potom, že grupy $pg_1(a,2b)$ a $pg_2(a,b)$ sú izomorfné. Veľkosti oboch grúp sú $4ab$, teda spĺňajú prvú podmienku. Ešte musíme nájsť izomorfizmus.

Majme predpis:

$$\begin{aligned} \phi : pg_1(a',b') &\longrightarrow pg_2(a,b) \\ \phi : P &\longmapsto P' \\ \phi : Q &\longmapsto Q'P'^{-1}Q'. \end{aligned}$$

Musíme ukázať, že je to skutočne homomorfizmus. Musíme overiť, že relácie $\phi(P)^2\phi(Q)^{-1} = (\phi(P)^{-1}\phi(Q))^a = (\phi(P))^{2b} = 1$ skutočne platia.

$$\phi(1) = \phi(P^2Q^{-2}) = \phi(P)^2\phi(Q)^{-2} = P'^2Q'^{-1}P'Q'^{-1}Q'^{-1}P'Q'^{-1} = P'^2Q'^{-2} = 1$$

v tomto bode využívame, že P'^2 v grupe $pg_2(a,b)$ patrí do centra a že $P'^2 = Q'^2$

$$= \phi((P^{-1}Q)^{a'}) = (\phi(P)^{-1}\phi(Q))^{a'} = (P'^{-1}Q'P'^{-1}Q')^{a'} = (P'^{-1}Q')^{2a'} = (P'^{-1}Q')^{2a} = 1$$

z prezentácie (16) vieme, že $(P'^{-1}Q')^aP'^{2b} = P'^{4b} = 1$, potom $(P'^{-1}Q')^a$ je involúcia

$$= \phi(P^{2b'}) = \phi(P)^{2b'} = P'^{2b'} = P'^{4b} = 1$$

Aby sme ukázali, že je to izomorfizmus, dokážeme, že každý prvok v grupe $pg_2(a,b)$ má vzor v grupe $pg_1(a',b')$. Do podgrupy $Im(\phi)$ patria prvky P' a $Q'P'^{-1}Q'$, potom aj $(P'^{-1}Q')^2$. Vzhľadom na to, že a je nepárne, platí $(P'^{-1}Q')^{2\frac{a+1}{2}} = P'^{-1}Q'P'^{2b}$. Potom ale do $Im(\phi)$ patrí aj $P'^{-1}Q'P'^{2b}P'^{-2b} = P'^{-1}Q'$ a teda aj $P'P'^{-1}Q' = Q'$. Podgrupa obrazov zobrazenia ϕ je generovaná prvkami P', Q', potom $Im(\phi) = pg_2(a,b)$.
čbtd

Na dokázanie opačnej implikácie by sme potrebovali nájsť počty na seba kolmých prvkov.

Teraz si uvedieme posledný z izomorfizmov, ktorý ale nemáme dokázaný, preto ho uvádzame len ako hypotézu:

Grupy $cm_2(a,b)$ a $pm_2(b,a)$ sú izomorfné práve vtedy, keď číslo $gcd(a,b)$ je nepárne.

Dôkaz implikácie zľava doprava ide cez štruktúru centier, tá ťažšia práca je nájsť daný izomorfizmus. My sme našli síce niekoľko homomorfizmov, ale žiaden sa napokon neukázal byť bijektívny, prípadne boli dané zobrazenia surjektívne, ale len pre niektoré špeciálne prípady parametrov.

Samozrejme by sa našli ešte ďalšie z izomorfizmov medzi nami skúmanými kvocientovými grupami, ich hľadanie však výrazne presahuje naše časové i rozsahové možnosti.

Použitá literatúra

I. Šuch, O.: Vertex - transitive maps on a torus. 2008

II. Lang, S.: Algebra. 1993. Addison - Wesley publishing company. ISBN 0-201-55540-9.

III. Šedivý, O.; Cuninka, A.: Základy elementárnej geometrie. 1989. Slovenské pedagogické nakladateľstvo. str. 68 - 90

IV. Mac Lane, S.; Birkhoff, G.: Algebra. 1974. Alfa.

V. Znám, Š.: Teória čísel. 1986. Alfa.

VI. Birkhoff, G.; Mac Lane, S.: Prehľad modernej algebry. 1979. Alfa.

VII. http://en.wikipedia.org/wiki/Wallpaper_group