UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Jan Kralj

Grigorčukova grupa in Burnsideov problem

Delo diplomskega seminarja

Mentor: doc. dr. Aleš Vavpetič

Ljubljana, 2010

Kazalo

Povzetek

Glavna tema dela je predstavitev prve Grigorčukove grupe, predvsem njenih treh lastnosti, s katerimi podaja odgovor na Burnsideov problem: je vsaka končnogenerirana grupa, v kateri ima vsak element končen red, končna? Ker je definicija Grigorčukove grupe tesno povezana s konceptom neskončnih dreves, je velik del uvoda namenjen podrobnemu poznavanju teh dreves in preslikav (posebej avtomorfizmov), s katerimi se konstruira Grigorčukova grupa. Po definiciji grupe kot podgrupe v grupi avtomorfizmov dreves je večji del namenjen njenim najpomembnejšim lastnostim. V zadnjem delu so omenjene še druge lastnosti grupe, ki so v marsičem bolj pomembne, a spadajo na podiplomski študij matematike.

Abstract

The main purpose of the seminar is an introduction of the first Grigorchuk group, especially the three properties that answer the Burnside problem: is a finitely generated group, in which every element is of finite order, finite? As the definition of the group is closely related to infinite rooted trees, a large part of the paper investigates both these trees and automorphisms between them, as the Grigorchuk group is constructed using these automorphisms. After the definition of the group as a subgroup in the group of automorphisms, the work focuses on some of its most important properties. In conclusion, some other properties, in many ways much more important, are mentioned, however their analysis is a post-graduate topic.

Math. Subj. Class. (2010): 20-XX, 20Fxx
Ključne besede: Grigorčukova grupa, končnogenerirana grupa, periodična grupa, neskončna drevesa, avtomorfizmi
Keywords: Grigorchuk group, finitely generated group, periodic group, infinite trees, automorphisms

1. Burnsideov problem

Za korektno formulacijo Burnsideovega problema najprej potrebujemo dve preprosti definiciji.

Definicija 1.1. *Naj bo G grupa z enoto 1. Grupa G je* končnogenerirana*, če obstaja taka končna podmnožica $S \subset G$, da S generira G, torej da lahko vsak $g \in G$ dobimo z množenjem elementov iz S.*

Definicija 1.2. *Naj bo G grupa z enoto 1. Grupa G je*

- periodična*, če je vsak njen element končnega reda, torej če velja*

$$\forall g \in G \exists n \in \mathbb{N} : g^n = 1,$$

- periodična z omejenim eksponentom*, če velja*

$$\exists n \in \mathbb{N} \forall g \in G : g^n = 1.$$

Definicija periodične grupe z omejenim eksponentom izgleda zelo podobno definiciji periodične grupe, a je med obema pomembna razlika. Pri periodični grupi zahtevamo samo končni red n za vsak element, ne pa tudi, da je n kakorkoli omejen.

Primer 1. *Označimo z G grupo $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \dots$. Ta grupa ni periodična, saj element $(1, 1, 1, \dots)$ ni končnega reda.*

Zato poglejmo njeno podgrupo H, definirano kot grupo tistih elementov G, ki imajo od nekega mesta naprej same ničle. Jasno je, da je H res grupa: če ima element a na mestih od k-tega naprej same ničle in ima element b na mestih od l-tega naprej same ničle, ima element $a + b$ na mestih od $\max\{k, l\}$ same ničle.

Enostavno je tudi pokazati, da je grupa H periodična. Naj bo

$$h = (h_1, h_2, \dots, h_k, 0, 0, \dots) \in H$$

poljuben element grupe H, ki ima na $k+1$-tem mestu in vseh nadaljnih same ničle in naj bo $M = 2 \cdot 3 \cdot 4 \cdots k \cdot (k+1)$. Upoštevamo $h_k \in \mathbb{Z}_{k+1}$ in posledično $(k+1) \cdot h_k = 0$ in dobimo:

$$M \cdot h = (\frac{M}{2} \cdot 2 \cdot h_1, \frac{M}{3} \cdot 3 \cdot h_2, \dots, \frac{M}{k+1} \cdot (k+1) \cdot h_k, 0, 0, \dots) = (0, 0, 0, \dots).$$

Grupa H kljub periodičnosti ni periodična z omejenim eksponentom. Če definiramo e_k kot element, ki ima na k-tem mestu enico, na vseh ostalih pa ničle, je red tega elementa očitno kar $k + 1$. Torej za vsako naravno število n obstaja element (e_{n-1}) grupe H, da velja $e_{n-1}^n \neq 0$ in torej grupa ni periodična z omejenim eksponentom.

V primeru je bilo večkrat uporabljeno dobro znano dejstvo, ki sledi iz Lagrangevega izreka, namreč da za vsak element g končne grupe G z enoto 1 velja $g^{|G|} = 1$. To dejstvo je pomembno, saj nam pove, da je vsaka končna grupa (ki je očitno tudi končnogenerirana) periodična z omejenim eksponentom. Burnsideov problem, ki ga je prvič predstavil matematik William Burnside leta 1902, sprašuje po obratu te dokaj očitne implikacije. Že sam avtor je postavil dve vprašanji:

- Splošni Burnsideov problem: ali je vsaka končnogenerirana periodična grupa končna?
- Burnsideov problem: ali je vsaka končnogenerirana periodična grupa z omejenim eksponentom končna?

Na prvi pogled se mogoče zdi, kot da je odgovor na obe vprašanji *da*, saj, če je grupa končnogenerirana, lahko izbiramo samo med končno mnogo generatorji, ker pa so generatorji končnega reda, lahko navidez izberemo le končno mnogo kombinacij teh generatorjev. Temu zmotnemu pogledu botruje implicitna predpostavka komutativnosti, ki v Burnsideovem problemu ni privzeta. Res, če je grupa G, generirana z elementi $g_1, g_2, \ldots, g_k$, periodična in abelova, lahko vsak element iz G zapišemo kot $g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k}$, in to tako, da so vsi n_i manjši od neke konstante. Neskončnost katerekoli grupe, ki želi stati kot dokaz, da je odgovor na zgornja vprašanja negativen, torej mora biti tudi posledica njene nekomutativnosti, saj tako lahko iz malo elementov zgradimo ogromno kombinacij (že aba^{-1} je element, različen od b).

Kot že rečeno, bo pravi odgovor na Burnsideovo vprašanje, ne, dala Grigorčukova grupa. Obstaja več ekvivalentnih definicij te grupe, med katerimi je verjetno najlažja tista, ki za vizualizacijo uporablja neskončna dvojiška drevesa.

2. Drevesa reda k

V diskretni matematiki je drevo graf (množica vozlišč in povezav med njimi), ki zadošča preprostemu pogoju: za vsaki dve vozlišči mora obstajati natanko ena pot, ki vodi od ene do druge (pot je zaporedje vozlišč, kjer sta dve zaporedni vozlišči med sabo povezani s povezavo). Programersko pojmovanje dreves je malce bolj specifična oblika tega pogleda. V računalništvu se eno od vozlišč grafa odlikuje za koren, vsa ostala so njegovi potomci (vozlišča, povezana s korenom, so sinovi korena, vsak sin pa je povezan s svojimi sinovi). Vozlišču s samo enim sosedom (brez sinov) se pogosto reče list. Za konstrukcijo Grigorčukove grupe je bolj primeren drugi, programerski pogled na drevesa, a tudi tega je potrebno malce razširiti, še prej pa ponoviti.

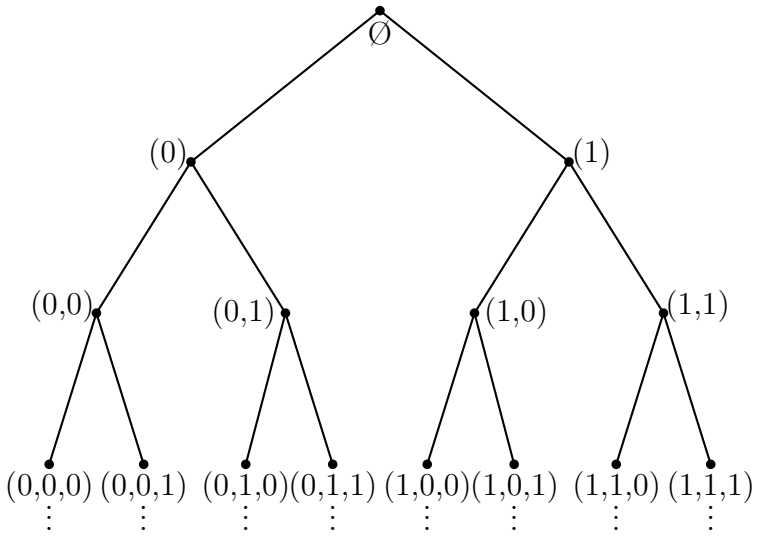
(1) Drevesa, ki nastopajo v programiranju, imajo pogosto lastnost, da je število sinov vozlišča omejeno. Tak primer so zelo pogosta dvojiška drevesa, v katerih ima vsako vozlišče največ tri, koren pa največ dva soseda (eden od sosedov vozlišča je tako njegov oče, ostala pa levi in desni sin). Koncept seveda ni omejen na število 2 in ga v splošnem lahko posplošimo na drevesa reda k, za katera velja, da ima vsako vozlišče največ $k+1$, koren pa največ k sosedov.

(2) Drevo reda k je polno, če ima zasedene vse nivoje do neke globine j. To pomeni, da ima vsako vozlišče, ki je od korena oddaljeno za manj kot j povezav (je na globini, manjši od j), k sinov, in da je vsako vozlišče na globini j list.

Čeprav to do sedaj ni bilo eksplicitno izraženo, so vsa drevesa, znana iz programiranja in diskretne matematike, končna (imajo končno mnogo vozlišč) in zato neprimerna za konstrukcijo kakršnekoli neskončne grupe. Razširitev pojma dreves tako prinaša natanko njihova neskončnost.

Definicija 2.1. Neskončno polno drevo reda k, *oznaka* $\mathcal{T}^{(k)}$, *je množica vseh končnih zaporedij števil iz množice* $\{0, 1, 2, \ldots, k-1\}$. *Vozlišče* $v = (v_1, v_2, \ldots, v_m)$ *je* sin *vozlišča* $u = (u_1, u_2, \ldots, u_n)$, *u pa je* oče *vozlišča v natanko tedaj, ko velja* $m = n+1$ *in* $\forall i \in \{1, 2, \ldots, n\} : v_i = u_i$. *Koren drevesa* $\mathcal{T}^{(k)}$ *je prazno zaporedje* $\emptyset$.

V definiciji smo torej poistovetili drevo kar s končnimi zaporedji izbranih naravnih števil in ničle. Ta koncept je enostaven za predstavo, saj nam tako poimenovana vozlišča drevesa pravzaprav povedo, kako do njih pridemo iz korena. Tako je pot



Slika 1. Neskončno drevo

od korena do vozlišča $(2, 5, 4, 2, 6)$ v drevesu reda najmanj 7 podana z zaporedjem vozlišč: $\emptyset, (2), (2, 5), (2, 5, 4), (2, 5, 4, 2), (2, 5, 4, 2, 6)$. Predstavljamo si lahko, da do tega vozlišča pridemo tako, da od korena najprej zavijemo na njegovega drugega sina, nato na petega, četrtega, drugega in nato šestega.

3. Avtomorfizmi

Čeprav je zgornja posplošitev grafov na neskončne objekte zadostila zahtevi po neskončnosti, je konstrukcija grupe še daleč, saj nikjer še nismo naleteli na strukturo kakršnekoli grupe. Težavi se hitro izognemo tako, da namesto samih grafov (oziroma dreves) gledamo preslikave med njimi. Že če vzamemo množico vseh preslikav iz $\mathcal{T}^{(k)}$ v $\mathcal{T}^{(k)}$ in kot operacijo med preslikavami opazujemo njihov kompozitum, ta množica zadosti aksiomom grupe, zato si lahko obetamo, da bomo nekje v tej veliki (preveliki) grupi našli tudi kakšno, ki bi bila zanimiva za opazovanje. Med vsemi preslikavami se zato najprej skoncentriramo na vse tiste, ki ohranjajo strukturo drevesa. Pojem izomorfizma grafov je sicer znan iz diskretne matematike in je torej definiran za končne grafe, vendar tega naša definicija pravzaprav sploh ne opazi.

Definicija 3.1. *Naj bosta Γ in Δ grafa.*
Bijektivna preslikava $f : \Gamma \to \Delta$ je izomorfizem grafov*, če za poljubni vozlišči u in v grafa Γ velja, da sta u in v povezani natanko tedaj, ko sta povezani $f(u)$ in $f(v)$. Preslikava je* avtomorfizem grafov*, če velja $\Gamma = \Delta$.*

Ker smo pojem sosednosti vozlišč definirali tudi za neskončna drevesa $\mathcal{T}^{(k)}$, lahko kot definicijo avtomorfizma neskončnih dreves vzamemo kar zgornjo definicijo. Pri tem hitro opazimo, da o izomorfizmih med drevesi različnih redov ni vredno izgubljati besed.

Trditev 3.2. *Vsak izomorfizem grafov ohranja število sosedov vozlišča.*
Naj bo $f : \Gamma \to \Delta$ izomorfizem grafov. Potem za vsako vozlišče v grafa Γ velja, da je točk, sosednjih vozlišču v, natanko toliko kot točk, sosednjih vozlišču $f(v)$.

Dokaz. Naj bodo $v_1, v_2, \ldots, v_n$ vsa vozlišča, sosednja v. Potem so vozlišča $f(v_1)$, $f(v_2), \ldots, f(v_n)$ sosednja $f(v)$ in jih je zaradi bijektivnosti f natanko n. Torej ima $f(v)$ vsaj toliko sosedov kot v. Ker je tudi f^{-1} izomorfizem grafov, ima tudi

$v = f^{-1}(f(v))$ vsaj toliko sosedov kot $f(v)$, kar pomeni, da imata tako $f(v)$ kot v natanko n sosedov. □

Posledica 3.3. *Naj bosta k in l neenaki naravni števili. Tedaj ne obstaja izomorfizem med drevesi $\mathcal{T}^{(k)}$ in $\mathcal{T}^{(l)}$.*

Dokaz. V drevesu $\mathcal{T}^{(k)}$ obstaja neskončno vozlišč s $k+1$ sosedi (takšna so vsa vozlišča razen korena). Če je $l = k+1$, je v drevesu $\mathcal{T}^{(l)}$ takšno vozlišče natanko eno (koren), sicer pa takšnega vozlišča v drevesu $\mathcal{T}^{(l)}$ sploh ni. V vsakem primeru je množica vozlišč s $k+1$ sosedi v drevesu $\mathcal{T}^{(l)}$, kamor se mora bijektivno slikati neskončno vozlišč drevesa $\mathcal{T}^{(k)}$, končne moči, zato primerna bijektivna preslikava ne obstaja. □

Posledica 3.4. *Vsak avtomorfizem $f : \mathcal{T}^{(k)} \to \mathcal{T}^{(k)}$ slika koren v koren. Splošneje velja, da f ohranja globino vsakega vozlišča (njegovo oddaljenost od korena).*

Dokaz. Koren je edino vozlišče v $\mathcal{T}^{(k)}$, ki ima samo k sosedov, zato se mora nujno preslikati samo vase.
Ohranjanje globine je najlažje dokazati z indukcijo. Prvi nivo so vsa vozlišča, povezana s korenom. Ker se ta morajo slikati v vozlišča, povezana s korenom (sicer f ni avtomorfizem) mora veljati, da se slikajo v vozlišča, katerih globina je ena. Enak argument poskrbi tudi za indukcijski korak. □

Naslednji koncept dreves, ki se ga splača prenesti iz računalništva, so poddrevesa in z njimi povezani predniki. Ker smo za drevesa že definirali relacijo očeta, po analogiji z družinskimi vezmi definicija prednika verjetno ne bo presenetljiva.

Definicija 3.5. *Naj bo v vozlišče v poljubnem (končnem ali neskončnem) drevesu $\mathcal{T}$. Vozlišče w je* prednik *vozlišča v natanko tedaj, ko velja*

(1) *$w = v$ ali*
(2) *Obstaja w' vozlišče drevesa $\mathcal{T}$, da je w oče w' in je w' prednik vozlišča v.*

Prednik vozlišča v je torej (poleg vozlišča samega) njegov oče, oče njegovega očeta in tako naprej vse do korena. Tako jasno vidimo, da so v našem primeru, ko vozlišča predstavljamo z besedami, predniki vozlišča $v = (v_1, v_2, \ldots, v_n) \in \mathcal{T}^{(k)}$ natanko vozlišča $(v_1, v_2, \ldots, v_i)$ za $i \in \{1, 2, \ldots, n\}$ ter koren, ki ga predstavlja prazna beseda $\emptyset$. Sedaj lahko uvedemo še koncept poddreves, prav tako znan predvsem iz računalništva.

Definicija 3.6. Poddrevo s korenom v vozlišču v *je množica vseh vozlišč, katerih prednik je v, in povezav med njimi.*

Za nas bodo najpomembnejša poddrevesa s korenom v vozliščih globine 1. Ker se ta vozlišča naravno oštevilčijo kar s številom, ki nastopa v besedi, ki jih predstavlja, bomo tako označili tudi poddrevesa. Tako bomo z izrazom *i-to poddrevo* označili poddrevo s korenom v vozlišču (i). V primeru dvojiških dreves bomo šli še korak dlje in poddrevo s korenom v vozlišču (0) označili kot levo, poddrevo s korenom v vozlišču (1) pa kot desno poddrevo.
Koncept poddrevesa je v računalništvu uporaben predvsem zato, ker je poddrevo praviloma manjše od celotnega drevesa (razen če je vozlišče v kar koren). Za nas bo zanimivo ravno zato, ker v neskončnih drevesih temu ni tako. Vidimo namreč, da je drevo, ki se začne v poljubnem vozlišču v, označimo ga s $\mathcal{T}_v^{(k)}$, spet neskončno polno drevo reda k, sestavljeno pa je iz vseh vozlišč, katerih beseda se začne z besedo v. Če torej vsem vozliščem $\mathcal{T}_v^{(k)}$ pokrijemo prvih nekaj števil zaporedja,

bomo dobili natanko vse besede drevesa $\mathcal{T}^{(k)}$, poleg tega pa bomo tudi ohranili relacijo povezanosti, saj nikoli ne pokrivamo zadnjih znakov (ti so edini, ki vplivajo na povezanost vozlišč). Pokazali smo torej, da je drevo $\mathcal{T}_v^{(k)}$ izomorfno drevesu $\mathcal{T}^{(k)}$. Izomorfizem med njima najlažje predstavimo z izomorfizmom:

$$\delta_v : \mathcal{T}^{(k)} \to \mathcal{T}_v^{(k)} \delta_v : x \mapsto vx,$$

kjer je vx beseda, ki jo dobimo s konkatenacijo besed v in x.

4. Stabilizatorske podgrupe

Ker so poddrevesa drevesa $\mathcal{T}^{(k)}$ tako zelo podobna osnovnemu drevesu (po naših kriterijih so mu pravzaprav enaka), se nam lahko zazdi smiselno, da bi avtomorfizem celega drevesa predstavili z njegovim delovanjem na posameznih poddrevesih. Za takšno predstavitev so zanimivi predvsem tisti avtomorfizmi, ki na nekem nivoju in nad njim delujejo kot identiteta.

Definicija 4.1. *Naj bo $G^{(k)}$ grupa vseh avtomorfizmov drevesa $\mathcal{T}^{(k)}$ in naj bo $L^{(k)}(d)$ množica vseh vozlišč globine d.* Stabilizatorska grupa $G^{(k)}$, ki ohranja nivo d, *oznaka $St_{G^{(k)}}(d)$ je grupa vseh tistih elementov $G^{(k)}$, ki na $L^{(k)}(d)$ delujejo kot identiteta, torej*

$$St_{G^{(k)}}(d) = \{g \in G^{(k)} : \forall x \in L^{(k)}(d) : g(x) = x\}.$$

Hitro lahko vidimo, da vsak avtomorfizem, ki ohranja vozlišče x, mora ohranjati tudi vse njegove prednike (najlažje to vidimo pri očetu x, saj se ta mora preslikati v natanko tistega soseda vozlišča $g(x) = x$, ki ima, to vemo iz prejšnjega poglavja, globino za eno manjšo od x, takšno vozlišče pa je samo eno, oče x-a. Za ostale prednike velja natanko isti premislek). Iz tega enostavno sledi, da vsak element grupe $St_{G^{(k)}}(d)$ ohranja ne le nivo d, ampak tudi vse nivoje pred njim, torej velja (zadnja enakost sledi iz dejstva, da vsak avtomorfizem ohranja koren)

$$St_{G^{(k)}}(d) \subset St_{G^{(k)}}(d-1) \subset \cdots \subset St_{G^{(k)}}(1) \subset St_{G^{(k)}}(0) = G^{(k)}.$$

Trditev 4.2. *Za vsak n je grupa $St_{G^{(k)}}(n)$ podgrupa edinka v $G^{(k)}$.*

Dokaz. Vzemimo poljuben $s \in St_{G^{(k)}}(n)$ in poljuben $g \in G^{(k)}$. Pokazati želimo, da tudi gsg^{-1} leži v $St_{G^{(k)}}(n)$. Vzemimo poljubno vozlišče v na globini n, torej $v = (v_1, v_2, \ldots, v_n)$ in si poglejmo, kam ga slika gsg^{-1}. Upoštevamo, da g^{-1} in g ohranjata globino, torej $g^{-1}(v) = (w_1, w_2, \ldots, w_n)$, in dobimo

$$gsg^{-1}(v) = g(s(g^{-1}(v))) = g(s(w_1, w_2, \ldots, w_n)).$$

Sedaj upoštevamo, da s na vsa vozlišča globine n deluje kot identiteta, zato je dalje

$$gsg^{-1}(v) = g(w_1 w_2 \ldots, w_n) = v,$$

kar pomeni $gsg^{-1} \in St_{G^{(k)}}(n)$. Ker za vsak element $g \in G^{(k)}$ velja, da iz $s \in St_{G^{(k)}}(n)$ sledi $gsg^{-1} \in St_{G^{(k)}}(n)$, je trditev dokazana (velja $\forall g \in G^{(k)} : gSt_{G^{(k)}}(n)g^{-1} = St_{G^{(k)}}(n)$). □

Za naše potrebe bo še posebno zanimiva stabilizatorska grupa, ki ohranja prvi nivo, to je $St_{G^{(k)}}(1)$. Za poljuben element iz te grupe velja, da ohranja vsa vozlišča globine 1 (in 0). Iz tega sledi preprosta trditev.

Trditev 4.3. *Naj bo g avtomorfizem iz stabilizatorske podgrupe, ki ohranja prvi nivo. Tedaj za vsako vozlišče $v = (v_1, v_2, \ldots, v_n)$ drevesa $\mathcal{T}^{(k)}$ velja*

$$g(v) = (v_1, w_2, w_3, \ldots, w_n).$$

Dokaz. Naj bo $g(v) = (w_1, w_2, w_3, \ldots, w_n)$ Vozlišče $v' = (v_1, v_2, \ldots, v_{n-1})$, je oče vozlišča v. To vozlišče se slika v tisto vozlišče na nivoju $n-1$ (ker avtomorfizem ohranja globino), ki je povezano z vozliščem $g(v)$, takšno vozlišče pa je samo oče vozlišča $g(v)$, to je $(w_1, w_2, \ldots, w_{n-1})$. Velja torej $g(v') = (w_1, w_2, \ldots, w_{n-1})$. Premislek nam po indukciji pove, da se vsi predniki vozlišča v slikajo v prednike vozlišča $g(v)$, posledično pa se vozlišče (v_1) slika v vozlišče (w_1). Ker vemo, da avtomorfizem g vozlišče (v_1) slika v isto vozlišče (sicer g ne bi ohranjal prvega nivoja), vidimo, da velja $(v_1) = (w_1)$, torej tudi $v_1 = w_1$, kar dokazuje trditev. □

Čeprav je dokaz trditve preprost, ima za razumevanje grupe $St_{G^{(k)}}(1)$ velik pomen. Trditev nam namreč pove, da delovanje avtomorfizma iz grupe $St_{G^{(k)}}(1)$ ohranja ne le zgornjih nekaj vozlišč, ampak tudi za vsa ostala vozlišča ohranja poddrevo, v katerem se nahajajo. To pomeni, da je avtomorfizem $g \in St_{G^{(k)}}(1)$, zožen na eno od poddreves, še vedno dobro definirana bijektivna preslikava in posledično tudi avtomorfizem. Videli smo torej, da vsak avtomorfizem $g \in St_{G^{(k)}}(1)$ pravzaprav poda k različnih avtomorfizmov, ki delujejo na primernih poddrevesih.

Lahko razmislek tudi obrnemo? Lahko za poljubno k-terico avtomorfizmov g_1, $g_2, \ldots, g_k \in G^{(k)}$ najdemo tak avtomorfizem $g \in St_{G^{(k)}}(1)$, da bo g na i-to poddrevo deloval kot avtomorfizem g_i? Odgovor je očitno *da*, saj iz zgornje trditve sledi, da delovanje avtomorfizma iz $St_{G^{(k)}}(1)$ na vsakem od poddreves že enolično določa ta avtomorfizem.

Ugotoviti moramo le še to, kam avtomorfizem g slika poljubno vozlišče $v = (v_1, v_2, \ldots, v_n)$. To vozlišče je v v_1-tem poddrevesu, kjer je z izomorfizmom $\delta_{(v_1)}$ v bijektivni zvezi z vozliščem $\delta^{-1}_{(v_1)}(v) = (v_2, v_3, \ldots, v_n)$ (vozlišče $(1,2,3)$ v trojiškem drevesu je pravzaprav vozlišče $(2,3)$ v njegovem prvem poddrevesu). Na v_1-to poddrevo deluje avtomorfizem g_{v_1}, kar pomeni, da se vozlišče $\delta^{-1}_{(v_1)}(v)$ slika v vozlišče $g(\delta^{-1}(v))$ v v_1-tem poddrevesu, ki pa je v originalnem drevesu pravzaprav vozlišče $\delta_{(v_1)} \circ g \circ \delta^{-1}_{(v_1)}(v)$.

Našli smo torej bijektivno preslikavo med vsemi k-tericami avtomorfizmov iz grupe $G^{(k)}$ in stabilizatorsko grupo $St_{G^{(k)}}(1)$. Ta preslikava je pomembna in si zasluži tudi svojo oznako.

Definicija 4.4. *Preslikava*

$$\psi : St_{G^{(k)}}(1) \to G^{(k)} \times G^{(k)} \times \cdots \times G^{(k)}$$

je preslikava, ki vsakemu elementu $g \in St_{G^{(k)}}(1)$ priredi element $(g_1, g_2, \ldots, g_k)$, tako da je g_i zožitev delovanja avtomorfizma g na i-to poddrevo drevesa $\mathcal{T}^{(k)}$.

Preslikava ψ je torej zožitev poljubnega avtomorfizma na vsako od k poddreves, v drugo smer pa je $\psi^{-1}(g_1, g_2, \ldots, g_k)$ tisti avtomorfizem, ki na vozlišče v i-tem poddrevesu deluje kot $\delta_{(i)} g_i \delta^{-1}_{(i)}$.

Trditev 4.5. *Preslikava ψ je izomorfizem grup, kjer je operacija v $G^{(k)} \times G^{(k)} \times \cdots \times G^{(k)}$ po komponentah.*

Dokaz. Imejmo avtomorfizma g in h iz grupe $St_{G^{(k)}}(1)$ in naj bo $\psi(g) = (g_1, g_2, \ldots, g_k)$ in $\psi(h) = (h_1, h_2, \ldots, h_k)$. Radi bi pokazali, da velja

$$\psi(gh) = \psi(g)\psi(h) = (g_1h_1, g_2h_2, \ldots, g_kh_k).$$

Vemo, da je h_i zožitev preslikave h na i-to poddrevo in g_i zožitev g na i-to poddrevo, hkrati pa vemo, da je i-ta komponenta $\psi(gh)$ enaka zožitvi avtomorfizma gh na i-to poddrevo. Radi bi torej pokazali enakost

$$gh|_1 = g|_1h|_1.$$

Ta enakost pravzaprav sledi iz dejstva, da sta g in h elementa $St_{G^{(k)}}(1)$. Ker sta oba avtomorfizma tudi bijekciji na prvo poddrevo, vrstni red njunega komponiranja in ožanja na to poddrevo ni pomemben. Preslikava h deluje na vsako vozlišče v v prvem poddrevesu natanko tako kot $h|_1$, preslikava g pa na vozlišče $h(v)$ (tu upoštevamo dejstvo, da je $h(v)$ v istem poddrevesu) natanko tako kot $g|_1$. Ker velja tudi, da je $g(h(v))$ element prvega poddrevesa, je $gh(v) = g|_1h|_1(v)$ za vsako vozlišče v prvem poddrevesu, kar dokazuje zgornjo enakost. Enak premislek velja za ostala poddrevesa, zato je trditev že dokazana. □

5. Avtomorfizmi a, b, c in d

Da ima grupa $G^{(k)}$ neko podgrupo, ki je izomorfna $G^{(k)} \times G^{(k)} \times \cdots \times G^{(k)}$, je mogoče nenavadno, vsekakor pa zanimivo. Takojšnja posledica tega dejstva je, da, ker v $G^{(k)} \times G^{(k)} \times \cdots \times G^{(k)}$ obstaja podgrupa, izomorfna $G^{(k)}$, takšna grupa obstaja tudi v $St_{G^{(k)}}(1)$, ta grupa pa je prava podgrupa v $G^{(k)}$. Posledično smo pokazali, da v $G^{(k)}$ obstaja neka prava podgrupa, ki je izomorfna $G^{(k)}$. To seveda že pomeni, da je grupa $G^{(k)}$ neskončne moči, kar nas ne bi smelo presenetiti. Kljub temu pa si je zgornji premislek vredno zapomniti.
Konstruirali smo torej neko neskončno grupo, za katero pa si ne moremo obetati, da bi bila končnogenerirana. V iskanju našega primera končnogenerirane periodične neskončne grupe se bomo morali torej poglobiti v eno od podgrup grupe $G^{(k)}$. V prvem koraku se bomo iz splošnih dreves reda k omejili le še na polna dvojiška neskončna drevesa, kakršno je na sliki 1. Sedaj si pogled omejimo še na 4 posebne elemente v grupi $G^{(2)}$.

Definicija 5.1. *Naj bo $\overline{1} = 0$ in $\overline{0} = 1$. Naj bo $v = (v_1, v_2, \ldots, v_n) \in \mathcal{T}^{(2)}$. Tedaj je $a \in G^{(2)}$ tisti avtomorfizem, za katerega velja $a(v) = (\overline{v_1}, v_2, \ldots, v_n)$.*

Avtomorfizem a je torej tisti avtomorfizem, ki levo poddrevo prestavi na desno stran, desno poddrevo pa na levo stran. Bolj zapletena je konstrukcija naslednjih treh avtomorfizmov.

Definicija 5.2. *Avtomorfizmi b, c in d so tisti elementi grupe $St_{G^{(2)}}(1)$, za katere velja:*

$$b = \psi^{-1}(a, c),$$
$$c = \psi^{-1}(a, d),$$
$$d = \psi^{-1}(1, b),$$

kjer 1 označuje identično preslikavo (ta je hkrati tudi enota v grupi $G^{(2)}$).

Ker je preslikava ψ izomorfizem (torej preslikava med dvema grupama, ki sta si pravzaprav enaki), se bomo od sedaj naprej njenemu pisanju izogibali, čeprav bo ta preslikava implicitno še vedno prisotna. Tako bomo namesto $b = \psi^{-1}(a, c)$ pisali

kar $b = (a, c)$, kar pomeni, da je b tisti avtomorfizem, ki ohranja prvi nivo (to vemo, ker ψ^{-1} slika v $St_{G^{(2)}}(1)$), na levo (drevesa v dvojiškem se, raje kot na ničto in prvo, delijo na levo in desno) poddrevo deluje z avtomorfizmom a, na desno pa z avtomorfizmom c.
Čeprav smo oznake poenostavili na

$$b = (a, c),$$
$$c = (a, d),$$
$$d = (1, b),$$

v definiciji treh avtomorfizmov ostaja neka navidezna cikličnost, zaradi katere definicija izgleda slabo definirana. Izgleda namreč, kot da je b definiran preko avtomorfizma c, c preko d, ta pa je definiran preko avtomorfizma b, ki je torej definiran preko samega sebe. Temu na srečo ni tako, saj je v definiciji skrito dejstvo, da je b tisti avtomorfizem, ki na **spodnji** nivo deluje z avtomorfizmoma a in c, medtem ko prvi nivo pušča nedotaknjen. V tem pogledu definicija torej ni ciklična, ampak samo rekurzivna. To ni težava, saj so vsa vozlišča predstavljena s končnimi besedami. Najlepšo predstavo o delovanju avtomorfizmov b, c in d nam da slika 2. Poglejmo še, kam ti avtomorfizmi preslikajo neko konkretno vozlišče, denimo $v = (1, 1, 0, 1, 0)$.

(1) Homomorfizem b je element $St_{G^{(2)}}(1)$, zato vemo, da ohranja prvo število v besedi ($b(v) = (1, \dots)$). Hkrati vemo, da je vozlišče v element *desnega* poddrevesa (v je dejansko vozlišče $(1, 0, 1, 0)$ v desnem poddrevesu). To pomeni, da b na vozlišče (besedo $(1, 0, 1, 0)$) deluje z avtomorfizmom c in torej velja $b(v) = (1, c(1, 0, 1, 0))$. Premislek nato ponovimo za avtomorfizem c, ki nujno ohranja prvo število v besedi $(1, 0, 1, 0)$. Torej je $b(v) = (1, 1, d(0, 1, 0))$, saj je vozlišče $(1, 0, 1, 0)$ vozlišče $(0, 1, 0)$ v desnem poddrevesu, na katerega deluje avtomorfizem c. V naslednjem koraku premisleka dobimo $b(v) = (1, 1, 0, 1(1, 0))$, saj d na desno poddrevo deluje z identiteto. Za identiteto seveda vemo, kam slika poljubno vozlišče, zato zaključimo $b(v) = (1, 1, 0, 1, 0) = v$

(2) Podoben premislek kot zgoraj nam za avtomorfizem c in vozlišče v pove:

$$c(v) = c(1, 1, 0, 1, 0) = (1, d(1, 0, 1, 0)) =$$
$$= (1, 1, b(0, 1, 0)) = (1, 1, 0, a(1, 0)) = (1, 1, 0, 0, 0).$$

(3) Razmislek ponovimo še z avtomorfizmom d:

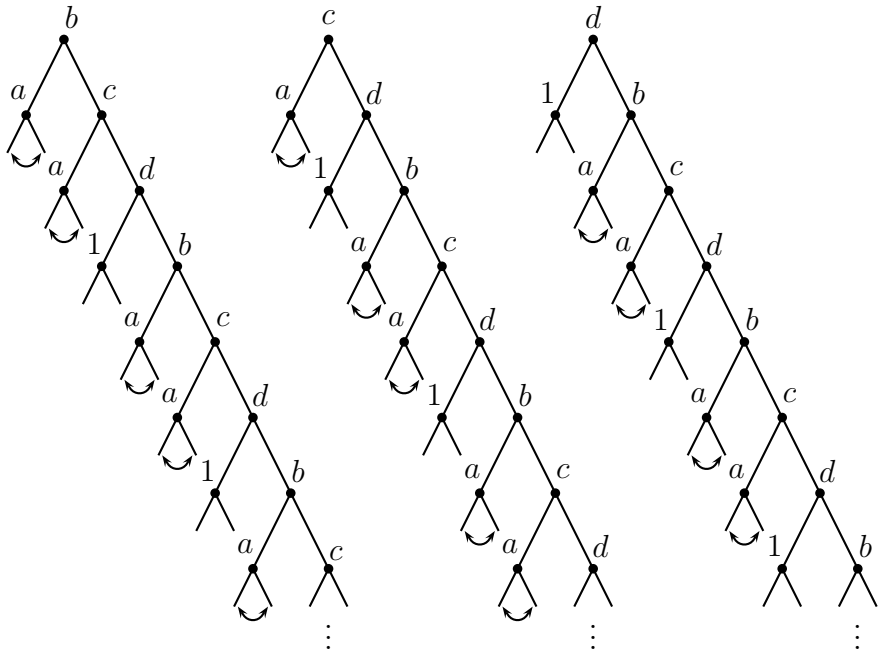
$$d(v) = d(1, 1, 0, 1, 0) = (1, b(1, 0, 1, 0)) =$$
$$= (1, 1, c(0, 1, 0)) = (1, 1, 0, a(1, 0)) = (1, 1, 0, 0, 0).$$

6. Prva Grigorčukova grupa

Po dolgih in napornih pripravah smo končno prišli do točke, kjer imamo vse potrebno za definicijo grupe, ki da odgovor na Burnsideovo vprašanje izpred 108 let.

Definicija 6.1. Prva Grigorčukova grupa Γ *je podgrupa grupe* $G^{(2)}$*, ki jo generirajo avtomorfizmi* a*,* b*,* c *in* d*.*
Krajše: $\Gamma = \langle a, b, c, d \rangle$*.*

Spomnimo se, da mora grupa Γ zadoščati trem lastnostim. Mora biti končnogenerirana, neskončna in periodična. Da jo generira končno mnogo generatorjev, ni



Slika 2. Delovanje avtomorfizmov b, c in d

potrebno dokazovati, saj je grupa že v definiciji generirana s štirimi svojimi elementi (v resnici celo velja, da za definicijo zadostujejo trije med njimi). Manj trivialen bo dokaz, da je grupa tudi neskončna, za kar si moramo natančneje pogledati že znani izomorfizem ψ iz $St_{G^{(2)}}(1)$ v $G^{(2)} \times G^{(2)}$. Ker nas ne zanima več celotna grupa $G^{(2)}$, ampak le še Γ, moramo primerno zožiti tudi stabilizatorsko grupo, ki jo opazujemo. Smiselno je, da se skoncentriramo na stabilizatorsko podgrupo grupe Γ, torej:

Definicija 6.2. Stabilizatorska grupa grupe Γ, ki ohranja prvi nivo, *je definirana kot* $St_\Gamma(1) = St_{G^{(2)}}(1) \cap \Gamma$.

Očitno je $St_\Gamma(1)$ grupa, saj je presek dveh grup, in torej podgrupa grupe Γ. Je tudi podgrupa edinka, saj je takšna $St_{G^{(2)}}(1)$, s preseki pa se ta lastnost deduje. Ker je avtomorfizem a element grupe Γ, ne pa tudi grupe $St_{G^{(2)}}(1)$, je $St_\Gamma(1)$ tudi prava podgrupa Grigorčukove grupe. Spomnimo se, da smo neskončnost osnovne grupe $G^{(2)}$ dokazovali z izomorfizmom ψ. Tega lahko brez težav zožimo (namesto na $St_{G^{(2)}}(1)$ zožitev slika le še iz $St_\Gamma(1)$), bolj zanimivo pa bo videti, kako se s tem spremeni slika preslikave. Za analizo tega si moramo najprej pobližje pogledati lastnosti enega od generatorjev grupe, avtomorfizma a.

6.1. **Avtomorfizem** a**.** Čeprav $a \in \Gamma$ deluje kot edini avtomorfizem, o katerem ni vredno izgubljati besed, temu ni povsem tako. Res je sicer, da je njegovo delovanje na vozliščih dvojiškega drevesa preprosto, a ker nas zanima njegovo obnašanje v grupi, to ni pomembno. Zanimajo nas torej predvsem lastnosti elementa a grupe Γ in ne lastnosti preslikave a na dvojiškem drevesu.

Trditev 6.3. *Red elementa* a *je* 2*, torej*

$$a^2 = 1.$$

Dokaz. Ker velja $\overline{\overline{1}} = 0$ in $\overline{\overline{0}} = 1$, je povsem jasno, da za poljubno vozlišče $v = (v_1, v_2, \ldots, v_n)$ velja

$$a^2(v) = a(a(v_1, v_2, \ldots, v_n)) = a(\overline{v_1}, v_2, \ldots, v_n) = \\ = (\overline{\overline{v_1}}, v_2, \ldots, v_n) = (v_1, v_2, \ldots, v_n) = v.$$

Avtomorfizem a^2 je torej tisti avtomorfizem, ki vsako vozlišče preslika samo vase, takšna pa je samo enota oziroma identiteta. □

Dokazana trditev je res povsem preprosta, a ima vseeno vsaj eno posledico, ki jo je vredno omeniti. Ker je $a^2 = 1$, namreč velja tudi $a^{-1} = a$, posledično pa je konjugiranje z elementom a kar množenje z a z leve in z desne.

Trditev 6.4. *Naj bo $g \in \Gamma$. Torej se da g napisati kot produkt generatorjev grupe Γ, $g = g_1 g_2 \ldots g_n$, kjer je $g_i \in \{a, b, c, d\}$ za vsak $i \in \{1, 2, \ldots, n\}$. Velja*

$$g \in St_\Gamma(1) \iff \textit{Število elementov } g_i\textit{, enakih } a\textit{, je sodo.}$$

Dokaz. Za dokaz trditve je najpomembnejše dejstvo, da so avtomorfizmi b, c in d vsi elementi $St_\Gamma(1)$. To seveda pomeni, da je v primeru, da noben g_i ni enak a, trditev že dokazana. Naj bo v vozlišče globine 1, torej $v = (v_1)$, kjer je $v_1 \in \{0, 1\}$. Ko nanj delujemo z avtomorfizmom g, nanj najprej deluje avtomorfizem g_n. Če je ta enak a, se v spremeni v $(\overline{v_1})$, sicer pa v (v_1). Vidimo, da se število v_1 spremeni v $\overline{v_1}$ (se konjugira) natanko tedaj, ko je g_n enak a, sicer pa ostane nespremenjeno. Razmislek ni omejen samo na g_n, ampak velja za vsak g_i, torej se v_1 konjugira natanko tolikokrat, kolikor je v besedi g elementov a.
Upoštevamo samo še očitno lastnost, da je k-krat konjugiran v_1 enak v_1 natanko tedaj, ko je k sodo število, in zaključimo, da je prvo število v besedi, ki predstavlja v, enako v_1 natanko tedaj, ko je število g_i, enakih a, sodo. Hkrati velja, da je $g \in St_\Gamma(1)$ natanko tedaj, ko vsakemu vozlišču ohranja prvo število v besedi, kar dokazuje trditev. □

Vidimo, da ima a torej posebno vlogo med generatorji Γ, kar se bo pokazalo še večkrat. Med drugim je zanimivo tudi opazovati, kako na ostale generatorje deluje konjugiranje z elementom a (vemo namreč že, da je $a^{-1} = a$).

Trditev 6.5. *Za generatorje grupe Γ velja:*

(1) $aba = (c, a)$,
(2) $aca = (d, a)$,
(3) $ada = (b, 1)$.

Dokaz. Pokazali bomo samo prvo točko trditve, medtem ko se ostale dokažejo po povsem enakem principu.
Preden se lotimo dokaza trditve, se je potrebno prepričati, da je zgornja trditev sploh smiselna. Uporabili smo namreč skrajšani zapis za elemente stabilizatorske grupe, katere lahko predstavimo z njihovim delovanjem na levem in desnem poddrevesu, tako da bi formalno prva točka trditve morala biti $aba = \psi^{-1}(c, a)$. Seveda je to možno in smiselno samo, če je element aba v grupi $St_\Gamma(1)$, saj točno tja slika tudi ψ^{-1}. Tu nam priskoči na pomoč prejšnja trditev, saj za element aba velja, da v njegovi predstavitvi a nastopa sodo mnogokrat, kar pomeni $aba \in St_\Gamma(1)$.
Vzemimo poljubno vozlišče $v = (v_1, v_2, \ldots, v_n) \in \mathcal{T}^{(2)}$ in si poglejmo, kam ga slika

avtomorfizem aba.

$$aba(v) = a(b(a(v_1, v_2, \ldots, v_n))) = a(b(\overline{v_1}, v_2, \ldots, v_n)) = \quad \text{(upoštevamo definicijo } b\text{)}$$
$$= \begin{cases} a(\overline{v_1}, a(v_2, v_3, \ldots, v_n)) & ; \overline{v_1} = 0 \\ a(\overline{v_1}, c(v_2, v_3, \ldots, v_n)) & ; \overline{v_1} = 1 \end{cases}$$
$$= \begin{cases} (v_1, a(v_2, v_3, \ldots, v_n)) & ; v_1 = 1 \\ (v_1, c(v_2, v_3, \ldots, v_n)) & ; v_1 = 0 \end{cases}.$$

Hkrati zaradi strukture izomorfizma ψ vemo tudi, kako na v deluje avtomorfizem, ki ga označimo (c, a):

$$(c, a)(v) = \begin{cases} (v_1, c(v_2, v_3, \ldots, v_n)) & ; v_1 = 0 \\ (v_1, a(v_2, v_3, \ldots, v_n)) & ; v_1 = 1 \end{cases}.$$

Avtomorfizma aba in (c, a) se torej ujemata na poljubnem vozlišču, kar pomeni, da sta enaka. □

6.2. **Avtomorfizmi b, c in d.** Ob definiciji generatorjev Grigorčukove grupe smo najprej definirali avtomorfizem a, nato pa hkrati ostale tri avtomorfizme. Njihove definicije so si zelo podobne, zato se zdi smiselno, da si bodo elementi delili tudi nekatere lastnosti. Ena izmed njih je tudi red.

Trditev 6.6. *Red generatorjev b, c in d je 2, torej*

$$b^2 = c^2 = d^2 = 1.$$

Dokaz. V našem poenostavljenem načinu pisanja lahko pišemo

$$b^2 = (a, c)^2 = (a^2, c^2) = (1, c^2)$$
$$c^2 = (a, d)^2 = (a^2, d^2) = (1, d^2)$$
$$d^2 = (1, b)^2 = (1^2, b^2) = (1, b^2).$$

Tu smo potenciranje lahko prestavili na posamezne koordinate, ker je po že dokazanem ψ izomorfizem. Znova izgleda, kot da smo naleteli na cikličnost argumentov, saj bi brez težav pokazali enakost $b^2 = 1$, ko bi le vedeli, da velja $c^2 = 1$, in znova nas bo rešila rekurzivna narava definicij naših generatorjev. Ta naravno kliče po dokazu z matematično indukcijo. Vzemimo torej poljubno vozlišče $v = (v_1, v_2, \ldots, v_n)$ in pokažimo, da ga avtomorfizmi b^2, c^2 in d^2 slikajo samega vase.

(1) Kot je pri dokazih z indukcijo pogosto, v trivialnem primeru dokaz ni potreben. V primeru, da je n enak 1, iz $b^2, c^2, d^2 \in St_\Gamma(1)$ sledi, da avtomorfizmi ohranjajo vse besede dolžine 1, torej $b^2(v) = c^2(v) = d^2(v) = v$.

(2) Sedaj predpostavimo, da b^2, c^2 in d^2 ohranjajo vsa vozlišča globine $n - 1$, torej da so vsi trije elementi grupe $St_\Gamma(n - 1)$. Posledično vemo, da tudi vsem globljim vozliščem ne spreminjajo prvih $n - 1$ znakov v besedi, ki jih predstavlja. Sedaj ločimo dva primera.

   (a) Naj obstaja $i \leq n$, da je $v_i = 0$ in $v_j = 1$ za $j < i$. To pomeni, da je v element levega poddrevesa na nivoju $i - 1 < n$. Na nivoju $i - 1$ avtomorfizem b^2 deluje z enim od avtomorfizmov b^2, c^2 in d^2, s katerim, določa natančna globina. Ker je v vozlišče v levem poddrevesu vozlišča $(v_1, v_2 \ldots, v_{i-1})$, na levo drevo pa vsi trije kvadrati generatorjev delujejo z identiteto, to že pomeni, da v tem primeru velja $b^2(v) = v$, povsem enak argument pa da še enakosti $c^2(v) = v$ in $d^2(v) = v$.

(b) Naj bo $v = (1, 1, \ldots, 1)$. Ker že vemo, da b^2, c^2 in d^2 ohranjajo prvih $n-1$ znakov vsakega vozlišča, se lahko v slika samo v samega sebe ali pa v $\overline{v} = (1, 1, \ldots, 1, 0)$. Hkrati vemo, da se v $\overline{v}$ slika že $\overline{v}$, kar ob bijektivnosti b^2, c^2 in d^2 pomeni, da se v lahko slika le sam vase, torej $b^2(v) = c^2(v) = d^2(v) = v$.

□

Za vsaj štiri elemente grupe Γ torej že vemo, da so končnega reda. Čeprav so to ravno generatorji, na tem mestu vseeno še ne moremo sklepati tudi na periodičnost celotne grupe.
Druga pomembna lastnost generatorjev b, c in d se nanaša na njihovo interakcijo in bo (skupaj z zgoraj dokazano trditvijo) v veliko pomoč pri vseh nadaljnih dokazih.

Trditev 6.7. *Za generatorje b, c in d grupe Γ velja*

$$bc = cb = d,$$
$$bd = db = c,$$
$$cd = dc = b.$$

Dokaz. Kot metoda dokazovanja se pri rekurzivni definiciji znova ponuja indukcija. Vzemimo poljubno vozlišče $v = (v_1, v_2, \ldots, v_n)$. Trdimo, da se delovanje avtomorfizma d na vozlišče v ujema z delovanji avtomorfizmov bc in cd na v ter podobno za ostali dve enakosti.

(1) V primeru, ko je n enak 1, si podobno kot v prejšnjem dokazu spet pomagamo s stabilizatorsko grupo $St_\Gamma(1)$. Ker so njeni elementi b, c in d, so v njej tudi bc, bd, cd, cd, db in dc. Vsi ti avtomorfizmi torej v slikajo nazaj v v, torej se vsi avtomorfizmi tudi ujemajo med sabo.

(2) Predpostavimo, da enakosti iz trditve že veljajo za vsa vozlišča na globini $n-1$ (torej da se na vozliščih na globini $n-1$ avtomorfizem d ujema z avtomorfizmoma bc in cd, avtomorfizem c z avtomorfizmoma bd in db ter avtomorfizem b z avtomorfizmoma cd in dc). Oglejmo si samo, kako na vozlišče v deluje avtomorfizem bc. Ob upoštevanju definicij avtomorfizmov b in c dobimo

$$\begin{aligned} bc(v) &= b(c(v_1, v_2, \ldots, v_n)) \\ &= \begin{cases} b(v_1, d(v_2, v_3, \ldots, v_n)) & ; v_1 = 1 \\ b(v_1, a(v_2, v_3, \ldots, v_n)) & ; v_1 = 0 \end{cases} \\ &= \begin{cases} (v_1, cd(v_2, v_3, \ldots, v_n)) & ; v_1 = 1 \\ (v_1, aa(v_2, v_3, \ldots, v_n)) & ; v_1 = 0 \end{cases} \end{aligned}$$

Sedaj upoštevamo indukcijsko predpostavko, po kateri se avtomorfizem cd ujema z avtomorfizmom b na vseh vozliščih globine $n-1$, torej tudi na $(v_2, v_3, \ldots, v_n)$. Upoštevamo tudi $a^2 = 1$ in dobimo

$$\begin{aligned} bc(v) &= b(c(v_1, v_2, \ldots, v_n)) \\ &= \begin{cases} (v_1, b(v_2, v_3, \ldots, v_n)) & ; v_1 = 1 \\ (v_1, 1(v_2, v_3, \ldots, v_n)) & ; v_1 = 0 \end{cases} \\ &= (1, b)(v) = d(v). \end{aligned}$$

bc se torej ujema z d tudi na globini n. Enak postopek dokaže tudi ostale enakosti, kar zaključuje dokaz.

□

Posledica 6.8. *Grupa, ki jo generirajo avtomorfizmi b, c in d, je izomorfna kleinovi četverki.*

Dokaz. Zaradi zgornjih enakosti vidimo, da ima grupa $\langle b, c, d\rangle$ samo štiri elemente (poleg generatorjev še identiteto), saj z množenjem b, c in d med sabo lahko dobimo samo identiteto ali enega od teh treh elementov. Torej je $\langle b, c, d\rangle$ lahko izomorfna samo ciklični grupi $\mathbb{Z}_4$ ali kleinovi četverki K_4, saj sta to edini grupi moči 4. Ker v $\langle b, c, d\rangle$ ni nobenega elementa reda 4, kakršen je element $1 \in \mathbb{Z}_4$, je torej

$$\langle b, c, d\rangle \cong K_4.$$

□

O generatorjih grupe Γ sedaj vemo že toliko, da smo ugotovili, da jih je celo preveč. Iz zgornje trditve namreč očitno sledi, da lahko grupo generiramo že z avtomorfizmom a in poljubnima dvema avtomorfizmoma iz množice $\{b, c, d\}$. Kljub temu je analiza grupe veliko lažja z vsemi štirimi avtomorfizmi, saj iz vseh trditev lahko potegnemo nekaj uporabnih zaključkov o splošnem elementu grupe Γ. Vsak element g te grupe lahko zapišemo kot produkt generatorjev. Predstavimo ga z neko besedo s črkami g_i iz množice $\{a, b, c, d\}$, torej $g = g_1 g_2 \dots g_n$. Zaporedje $\{g_i\}_{i=1}^n$, ki določajo element g, je popolnoma poljubno, a ga z že pridobljenim znanjem o generatorjih mogoče lahko priredimo. Če namreč obstaja $i \in \{1, 2, \dots, n-1\}$, da je $g_i = g_{i+1}$, lahko besedo okrajšamo tako, da črki $g_i g_{i+1}$ preprosto črtamo oziroma zamenjamo z enoto. Podobno lahko storimo tudi, če obstaja nek $j \in \{1, 2, \dots, n-1\}$, da velja $g_j \in \{b, c, d\}$ in $g_{j+1} \in \{b, c, d\}$. Tedaj je namreč produkt generatorjev $g_j g_{j+1}$ po prejšnjem izreku tudi eden od generatorjev b, c ali d. Vsako besedo lahko okrajšamo tako, da

(1) noben od elementov ne nastopa dvakrat zapored (sicer to ponovitev "krajšamo", saj je enaka 1) in
(2) da je med poljubnima dvema elementoma vedno natanko eden enak a (sicer ju zmnožimo v en sam element).

Definicija 6.9. *Za vsak element $g \in \Gamma$ obstaja beseda $g_1 g_2 \dots g_n$, ki ga predstavlja in hkrati zadostuje zgornjima pogojema. To je* okrajšana *beseda, ki predstavlja g.*

Primer 2. *V zgornji definiciji je potrebno poudarjeno besedo prebrati res natančno. Beseda, ki zadostuje pogojema, je okrajšana, kar pa ne pomeni, da je tudi najkrajša. Naivni primer tega je poljuben element grupe $St_\Gamma(1)$, označimo ga g, ki na obe poddrevesi deluje z istim izomorfizmom x. Za ta element namreč velja $aga = g$, in čeprav je beseda aga daljša od g, sta obe besedi okrajšani. Ta argument nas seveda ne sme popolnoma prepričati, saj še vedno temelji na obstoju nekega hipotetičnega g. Zato si raje poglejmo element $(b, 1) \in St_\Gamma(1)$ ki ga po trditvi lahko predstavimo z besedo ada. Sedaj element z leve in z desne pomnožimo z $(1, b) = d$ in dobimo $d(ada)d = (1, b)(b, 1)(1, b) = (1b1, b1b) = (b, 1) = ada$. Pokazali smo torej, da besedi ada in $dadad$ predstavljata isti element, in čeprav sta obe okrajšani, je le ena izmed njiju tudi najkrajša.*

6.3. **Neskončnost.** Šele ko razumemo posebnosti generatorjev grupe Γ, se lahko posvetimo dokazu neskončnosti grupe. Pri tem nam bo v veliko pomoč predvsem trditev 6.5.

Trditev 6.10. *Slika preslikave $\psi|_{St_\Gamma(1)}$ je podgrupa v $\Gamma \times \Gamma$.*

Dokaz. Vzemimo poljuben element $g \in St_\Gamma(1)$, ki ga predstavlja okrajšana beseda $g = g_1 g_2 \dots g_n$. Ker je g element stabilizatorske podgrupe, mora veljati, da je število elementov g_i, enakih a, sodo. To pomeni, da je g oblike $xv_1av_2 \dots av_k y$, kjer sta x in y bodisi enota bodisi a, a v vsakem primeru lahko množenje, ki nas pripelje do elementa g, z oklepaji zapišemo tako, da množimo samo elemente iz $St_\Gamma(1)$. Če velja $x = y = a$, g zapišemo kot $g = (av_1a)v_2(av_3a)\dots(av_ka)$, v ostalih primerih pa postopamo podobno. V vsakem primeru to lahko storimo zato, ker je a-jev v besedi sodo mnogo, k vsakemu v_i pa "pripnemo"dva.
Sedaj poglejmo, kam se element g (samo v primeru $x = y = a$, saj so ostali analogni) slika z izomorfizmom ψ. Za $\psi(g)$ dobimo:

$$\psi(g) = \psi((av_1a)v_2(av_3a)\dots(av_ka)) = \\ \psi(av_1a)\psi(v_2)\psi(av_3a)\dots\psi(av_ka).$$

Ker (po trditvi 6.5) za vsak generator $v_i \in \{b, c, d\}$ velja $\psi(v_i) \in \Gamma \times \Gamma$, pa tudi $\psi(av_ia) \in \Gamma \times \Gamma$, je element $\psi(g)$ produkt samih elementov iz $\Gamma \times \Gamma$. To že pomeni $\mathrm{im}\psi|_{St_\Gamma} \subset \Gamma \times \Gamma$. Ker je tudi grupa, je trditev dokazana. □

Trditev 6.11. *Če izomorfizem ψ napišemo po komponentah kot $\psi = (\Phi_0, \Phi_1)$, sta*

$$\Phi_0, \Phi_1 : St_\Gamma(1) \to \Gamma$$

surjektivna homomorfizma grup.

Dokaz. Da sta obe preslikavi resnično homomorfizma, preprosto sledi iz trditve 4.5. Tam smo pokazali, da je produkt poljubnih avtomorfizmov (x, y) in (w, z) iz stabilizatorske grupe, ki ju predstavimo z njunim delovanjem na poddrevesih, enak (xw, yz). Ker množenje lahko prestavimo na komponente, sta Φ_0 in Φ_1 homomorfizma.
Za dokaz njune surjektivnosti se zopet obrnemo na trditev 6.5, iz katere sledijo enakosti:

$$\begin{array}{llll} \Phi_0(b) = a, & \Phi_0(aba) = c, & \Phi_1(b) = c, & \Phi_1(aba) = a, \\ \Phi_0(c) = a, & \Phi_0(aca) = d, & \Phi_1(c) = d, & \Phi_1(aca) = a, \\ \Phi_0(d) = 1, & \Phi_0(ada) = b, & \Phi_1(d) = b, & \Phi_1(ada) = 1. \end{array}$$

Ker tako Φ_0 kot Φ_1 poslikata vse generatorje grupe Γ, to že pomeni, da za vsak element Γ, ki je seveda produkt teh generatorjev, lahko najdemo element $St_\Gamma(1)$, ki se vanj slika. □

Spomnimo se, da je bila preslikava ψ, definirana na $St_{G^{(2)}}(1)$, izomorfizem med to grupo in grupo $G^{(2)} \times G^{(2)}$. Če preslikavo zožimo na Γ, smo pokazali, da ima ta še vedno nekaj lepih lastnosti. Njene komponente so surjektivne, od originalne preslikave podeduje tudi injektivnost, hkrati pa se je z oženjem definicijskega območja po pričakovanjih zožila tudi kodomena. Vse kaže, da lahko potegnemo popoln analog med celotno in zoženo preslikavo in ugotovimo, da je $\psi|_{St_\Gamma(1)}$ dejansko izomorfizem med $St_\Gamma(1)$ in $\Gamma \times \Gamma$. V ta razmislek nas zavede dejstvo, da je $\psi|_{St_\Gamma(1)}$ sestavljena iz dveh surjektivnih komponent, a zaključek je zavajujoč. Če bi hoteli pokazati, da je $\psi|_{St_\Gamma(1)}$ surjektivna, bi morali pokazati več kot trditev 6.11, saj bi morali najti avtomorfizme, ki se slikajo v vsakega od *osmih* generatorjev grupe $\Gamma \times \Gamma$, namreč $(a, 1)$, $(b, 1)$, $(c, 1)$, $(d, 1)$, $(1, a)$, $(1, b)$, $(1, c)$ in $(1, d)$. Da takšni avtomorfizmi ne obstajajo, najlažje pokažemo tako, da svoj pogled iz strukture grupe znova dvignemo na delovanje grupe na $\mathcal{T}^{(2)}$. Iz slike 2 je namreč jasno razvidno, da za $g \in \{b, c, d\}$ velja,

da lahko za vsak k najdemo neko vozlišče $v = (v_1, v_2, \ldots, v_k)$ globine k ali več, za katerega je $g(v) = (v_1, v_2, \ldots, \overline{v_k})$ (vozlišče se torej slika v svojega brata v hierarhiji drevesa). Če pokažemo, da to velja za vsak element $St_\Gamma(1)$, hkrati pa vidimo, da to ne velja za $\psi^{-1}(a, 1)$, bo iz tega sledilo, da $(a, 1) \in St_{G^{(2)}}(1)$ ni element $St_\Gamma(1)$. Posledično to pomeni, da se (zaradi injektivnosti ψ) noben element iz $St_\Gamma(1)$ s ψ ne slika v $(a, 1)$, kar že pomeni, da $\psi|_{St_\Gamma(1)}$ ne poslika celotne grupe $\Gamma \times \Gamma$.
Naj bo $g \in St_\Gamma(1)$ element, ki ga predstavlja okrajšana beseda $g_1 g_2 \ldots g_n$ dolžine n in naj bo $k \in \mathbb{N}$ poljuben.

(1) V primeru, ko je n enak 1, mora veljati $g \in \{b, c, d\}$, kar že pomeni, da zanj za vsako globino obstaja vozlišče te globine, ki se slika v svojega brata. Primer, ko je n enak 2, odpravimo še hitreje, saj vsaka okrajšana beseda dolžine 2 vsebuje natanko en a, kar pa pomeni, da element, ki ga ta beseda predstavlja, po trditvi 6.4 ni element grupe $St_\Gamma(1)$.
Tudi v primeru, ko je n enak 3, nimamo težkega dela. V tem primeru lahko v besedi g avtomorfizem a nastopa enkrat ali dvakrat. Po prejšnjem argumentu vidimo, da prva možnost odpade, možnost dveh pojavitev a pa nam izbor omeji na elemente aba, aca in ada. Ker ti elementi na vozlišča drevesa delujejo zelo podobno kot elementi b, c in d, le da zamenjajo levo in desno poddrevo, tudi v tem primeru lastnost velja.

(2) Predpostavimo sedaj, da trditev velja za vse avtomorfizme, ki jih predstavlja okrajšana beseda dolžine manj kot n. Ker je beseda, ki predstavlja g, okrajšana, vemo, da s premeščanjem oklepajev njegovo besedo lahko zapišemo v obliki, ki smo jo spoznali v trditvi 6.10, torej $g = (ag_2a)g_4(ag_6a)\ldots$ ali $g = g_1(ag_3a)g_5\ldots$ V vsakem primeru ga lahko zapišemo kot produkt največ $\frac{n+1}{2}$ elementov iz $St_\Gamma(1)$ (ki pa niso generatorji). To pomeni, da obstajata elementa $u, w \in St_\Gamma(1)$, da je $g = (u, w)$, hkrati pa lahko u in w predstavimo z besedama dolžine največ $\frac{n+1}{2}$. Ker za $n > 3$ velja $\frac{n+1}{2} < n$, lahko na u in w uporabimo indukcijsko predpostavko. Obstaja torej neko vozlišče $v = (v_1, v_2, \ldots, v_k)$, katerega w preslika v njegovega brata. Posledično bo g vozlišče $v' = (1, v_1, v_2, \ldots, v_k)$ preslikal v

$$(1, w(v_1, v_2, \ldots, v_k)) = (1, v_1, v_2, \ldots, \overline{v_k}),$$

torej v njegovega brata. Ker je vozlišče v' globine vsaj k, to dokazuje trditev. $\psi|_{St_\Gamma(1)}$ na žalost ne podeduje vseh lastnosti originalne preslikave.

Sedaj lahko pokažemo, da v sliki izomorfizma $\psi|_{St_\Gamma(1)}$ pravzaprav manjka še več generatorjev. Iz enakosti $(a, b) = (aaa, 1cd) = (a, 1)(a, c)(a, d)$ vidimo, da je avtomorfizem (a, b) v sliki, če je le v sliki tudi $(a, 1)$. Velja tudi obrat, saj velja $(a, 1) = (a, b)(a, d)^{-1}(a, c)^{-1}$. To pomeni, da bi iz $(a, b) \in \mathrm{im}\psi|_{St_\Gamma(1)}$ sledilo protislovje $(a, 1) \in \mathrm{im}\psi|_{St_\Gamma(1)}$, saj za $(a, c) = \psi(b)$ in $(a, d) = \psi(c)$ vemo, da ležita v $\mathrm{im}\psi|_{St_\Gamma(1)}$. Podobno lahko pokažemo, da sta zunaj $\mathrm{im}\psi|_{St_\Gamma(1)}$ tudi izomorfizma $(1, c) = (a, c)(a, 1)$ in $(1, d) = (a, d)(a, 1)$, premislek pa lahko ponovimo še za $(1, a)$, $(c, 1)$ in $(d, 1)$.
Čeprav je mogoče izgledalo razumljivo, da bo ψ ob zožitvi na $St_\Gamma(1)$ ohranil skoraj vse svoje koristne lastnosti, je bil začetni optimizem torej pretiran. Da $\psi|_{St_\Gamma(1)}$ ne nosi vseh lastnosti svojega "prednika", je pač posledica tega, da smo z ožanjem domene le to pravzaptav naredili bolj nenavadno, da bo lahko služila kot odgovor na začetno vprašanje, hkrati pa tudi manj "lepo". Vseeno nam bodo lastnosti, ki jih preslikava ψ podeduje, povsem zadostovale pri naslednji pomembni posledici.

Posledica 6.12. *Grupa* Γ *je neskončna.*

Dokaz. V trditvi 6.11 smo pokazali, da je slika homomorfizma Φ_0 enaka celotni grupi Γ. Moč domene, grupe $St_\Gamma(1)$, je torej večja ali enaka moči grupe Γ. Hkrati velja $a \notin St_\Gamma(1)$ in je torej $St_\Gamma(1)$ prava podgrupa grupe Γ. Grupa Γ torej vsebuje pravo podmnožico, katere moč je vsaj enaka moči Γ, zato tako kot za celotno grupo $G^{(2)}$ zaključimo, da je moč Grigorčukove grupe neskončna. □

6.4. **Periodičnost.** Grupa Γ torej zadošča vsaj dvema lastnostima, ki ju potrebuje, da odgovori na Burnsideovo vprašanje. Pokazati moramo le še zadnjo, in sicer da je vsak njen element končnega reda. Vemo že, da to velja za vse njene generatorje, a kot ponavadi iz tega ne smemo vleči prehitrih in nepremišljenih zaključkov. Dokaz, da so končnega reda vsi elementi in ne le generatorji, namreč ni preprost, hkrati pa je do zaključka težko priti preko mnogih manjših trditev, kot smo to storili do sedaj. Problema se je potrebno lotiti z grobo silo.

Definicija 6.13. *Grupa* G *je* 2*-grupa natanko tedaj, ko velja*

$$\forall g \in G \exists k \in \mathbb{N} : red(g) = 2^k.$$

Trditev 6.14. *Grupa* Γ *je* 2*-grupa.*

Dokaz. Vzemimo poljuben $g \in \Gamma$. Vemo, da g lahko predstavimo z okrajšano besedo, $g = g_1 g_2 \dots g_n$, kjer je $n \geq 1$ in $\forall i \leq n : g_i \in \{a, b, c, d\}$. Glede na dosedanji potek dokazov je verjetno že samoumevno, da bomo trditev dokazali s pomočjo indukcije po dolžini besede, ki predstavlja g.
Primer, ko je n enak 1, je zopet trivialen, saj smo potrebne enakosti dokazali že v prejšnjih trditvah. Zanimivo pa je pogledati tudi, kakšen je red elementov z besedo dolžine 2. To so besede ab, ac in ad ter njim konjugirani ba, ca in da. Dovolj je pogledati rede prvih treh elementov, saj so redi drugih treh enaki.

- Element ad. Najprej izračunamo $(ad)^2 = (ada)d = (b, 1)(1, b) = (b, b)$. Ker je $b^2 = 1$, je torej $(ad)^4 = (b^2, b^2) = (1, 1) = 1$. Red elementa ad (in njemu konjugiranega da) je torej 4, saj $(ad)^3$ ni element $St_\Gamma(1)$, kjer leži identiteta.
- Element ac. Spet pogledamo $(ac)^2 = (aca)c = (d, a)(a, d) = (da, ad)$. Upoštevamo prejšnjo točko in ugotovimo $(ac)^8 = ((ad)^4, (ad)^4) = (1, 1) = 1$. Red elementa torej deli 8, hkrati pa ne more biti manjši od 8, saj je $(ac)^4 = ((ad)^2, (ad)^2) = (b, b) \neq (1, 1)$.
- Element ab. Iz $(ab)^2 = (aba)b = (c, a)(a, c) = (ca, ac)$ in prejšnje točke tokrat izračunamo, da je $(ab)^{16} = ((ca)^8, (ac)^8)$, in ker $(ab)^{16} = (b, b)$ ni identiteta, zaključimo, da je red elementa ab enak 16.

Predpostavimo sedaj, da ima vsak element, ki ga predstavi beseda, krajša od n, red potenco števila 2. Takoj lahko ločimo dva primera.

(1) Število n je liho. Ker vemo, da je vsaka druga črka v besedi $g_1 g_2 \dots g_n$ enaka a, to pomeni bodisi $g_1 = g_n = a$ bodisi $g_1 \neq a$ in $g_n \neq a$.
   - Če velja $g_1 = g_n = a$, je element g oblike $g = aha$ za $h = g_2 g_3 \dots g_{n-1}$. Element g je torej konjugiran elementu, ki ga lahko predstavimo z besedo dolžine $n - 2$ in je po indukcijski predpostavki reda potence števila 2. Vemo, da ima vsak element enak red kot njemu konjugiran element, zato je takšen tudi element g.
   - Če sta tako g_1 kot g_n različna od a, postopamo podobno. Če velja $g_1 = g_n$, lahko ponovimo argument iz zgornje točke, v nasprotnem primeru

pa pogledamo element $h = g_1 g g_1$, ki je enakega reda kot g. Beseda, ki predstavlja h, sicer izgleda dolžine $n+2$, a če g razpišemo, vidimo $h = g_1 g_1 g_2 \dots g_n g_1 = g_2 g_3 \dots g_{n-1} x$ za nek $x \in \{b, c, d\}$. Pri tem smo upoštevali trditev 6.7, namreč da se poljubna 2 izmed generatorjev b, c in d (sem spadata tako g_1 kot g_n) zmnožita v tretjega. V vsakem primeru ima g torej enak red kot element, ki ga predstavlja beseda dolžine, manjše od n, in ima torej red potence števila 2.

(2) Število n je sodo, torej $n = 2k$ za nek $k \in \mathbb{N}$. Potem je g bodisi oblike $g = au_1 au_2 \dots au_k$ bodisi $g = u_1 au_2 a \dots u_k a$. Na srečo nam na tem mestu ni potrebno ločiti primerov, saj je v drugem primeru element aga, ki ima enak red kot g, oblike $aga = au_1 au_2 \dots au_k aa = au_1 au_2 a \dots u_k$. Brez škode za splošnost lahko predpostavimo, da se beseda, ki predstavlja g, začne z a. Zopet ločimo dva primera.

(a) Naj bo število k sodo. Ker v besedi $au_1 au_2 \dots au_k$ element a nastopa k-krat, to pomeni, da je g element grupe $St_\Gamma(1)$. Zapišemo ga lahko kot $g = (au_1 a)u_2(au_3 a) \dots (au_{k-1} a)u_k$, nato pa pogledamo, kam ga slika preslikava ψ. Dobimo

$$\begin{aligned}
&\psi(g) = \psi(au_1 a)\psi(u_2)\psi(au_3 a) \dots \psi(au_{k-1} a)\psi(u_k),\\
&\psi(g) = (x_1, y_1)(x_2, y_2) \dots (x_k, y_k) \text{za } x_i, y_i \in \{a, b, c, d\},\\
&\psi(g) = (x, y),
\end{aligned}$$

kjer sta x in y predstavljena z besedo dolžine največ l.
Znova lahko uporabimo indukcijsko predpostavko, saj sta x in y predstavljena z besedo, krajšo od n. Obstajata torej nek i in j, da je $red(x) = 2^i$ in $red(y) = 2^j$. Definiramo sedaj z kot najmanjši skupni večkratnik števil 2^i in 2^j (to število je kar $2^{\max\{i,j\}}$) in si poglejmo $\psi(g^z)$. Dobimo

$$\begin{aligned}
\psi(g^z) = \psi(g)^z = (x, y)^z = (x^z, y^z) =\\
= (x^{2^{\max\{i,j\}}}, y^{2^{\max\{i,j\}}}) = (1, 1),
\end{aligned}$$

in ker je ψ izomorfizem grup (ker je red elementa g v Γ enak kot v $G^{(2)}$, lahko gledamo prvotno, nezožano definicijo homomorfizma), lahko zaključimo $g^z = 1$. Hkrati iz teorije grup vemo, da iz $g^z = 1$ sledi, da red elementa g mora deliti z, in ker je z potenca števila 2, ga delijo le nižje potence števila 2. To pomeni, da je tudi red elementa g enak potenci števila 2.
Premislek pa lahko zaostrimo in pokažemo, da red g ne le deli z, ampak je kar enak z. Če bi bil red manjši, bi bil torej enak 2^m, kjer bi bil $m < i$ ali $m < j$. Tedaj bi iz enakosti g^{2^z} sledilo $x^{2^m} = 1$ (protislovje z $2^m < 2^i = red(x)$) in $y^{2^m} = 1$ (protislovje z $2^m < 2^j = red(y)$), obe možnosti pa vodita v protislovje.
Če je k sodo, je g torej reda $2^{\max\{i,j\}}$ in trditev velja.

(b) Naj bo število k liho. Ker je n sodo in si ne moremo pomagati s konjugiranjem, k pa je liho in element g ne leži v $St_\Gamma(1)$, izgleda, da bo naloga tu najtežja. Prvo dejstvo, ki nam bo pomagalo, je $g^2 \in St_\Gamma(1)$, saj beseda, ki predstavlja g^2, vsebuje sodo mnogo ponovitev a (besede gg se tudi ne da okrajšati, saj je prvi znak v g enak a, zadnji pa ne).

Na g^2 lahko ponovimo razmislek iz prejšnjih točk in ga napišemo kot

$$g^2 = ag_1ag_2 \dots ag_kag_1ag_2 \dots ag_k$$
$$g^2 = (ag_1a)g_2(ag_3a) \dots (ag_ka)g_1(ag_2a) \dots (ag_{k-1}a)g_k.$$

V našem poenostavljenem zapisu torej lahko napišemo $g^2 = (x, y)$, kjer sta x in y predstavljena z besedo dolžine največ $2k = n$. Navidez sedaj nismo pridobili nič, saj na x in y ne moremo uporabiti indukcijske predpostavke. Zato moramo znova (tokrat zadnjič) ločiti nekaj primerov.

- Denimo, da obstaja m, da je $g_m = d$. Vemo, da v besedi, ki predstavlja g^2, nastopa tako $g_m = (1, b)$ kot $ag_ma = (b, 1)$. Hkrati vemo, da lahko x zapišemo z besedo, v kateri po vrsti nastopajo avtomorfizmi, s katero g^2 deluje na levo poddrevo. To so torej natanko prve koordinate homomorfizma ψ, slike homomorfizma Φ_0. Velja torej $x = \Phi_0(ag_1a)\Phi_0(g_2) \dots \Phi_0(g_k)$, in ker je $\Phi_0(g_m) = \Phi_0(d) = 1$, to pomeni, da lahko x predstavimo z besedo dolžine največ $n - 1$. Hkrati zaradi enakosti $\Phi_1(ag_ma) = \Phi_1(ada) = 1$ enak zaključek lahko potegnemo tudi za avtomorfizem y. Znašli smo se torej v že znanem primeru, kjer g^2 predstavimo z dvema elementoma x in y, katerih red je potenca števila 2 ($red(x) = 2^i$, $red(y) = 2^j$). Natanko tako kot prej lahko pokažemo, da je red elementa g^2 enak večjemu od obeh redov. Hkrati pa to pomeni tudi $g^{2 \cdot 2^{\max\{i,j\}}} = 1$, torej $red(g)$ deli število $2^{\max\{i,j\}+1}$. Vemo, da ne more biti manjši od tega števila, saj bi to pomenilo, da bi se red zmanjšal tudi elementu g^2, kar pa vodi v protislovje. Red elementa g je torej enak natanko $2^{\max\{i,j\}+1}$.
- Denimo, da obstaja m, da je $g_m = c$. Z natanko enakim premislekom kot prej vidimo, da v besedi, ki predstavlja x, nastopa $\Phi_0(ag_ma) = \Phi_0(aca) = d$, v besedi, ki predstavlja y, pa nastopa $\Phi_1(g_m) = \Phi_1(c) = d$. Elementa x in y torej lahko predstavimo z besedama, ki vsebujeta vsaj eno ponovitev elementa d. Ti besedi sicer morda lahko še okrajšamo in s tem izgubimo element d, a v tem primeru že lahko uporabimo indukcijsko predpostavko. Če ju ne moremo okrajšati, si pomagamo z že dokazanim, saj smo za besede, ki vsebujejo ponovitev elementa d, v prejšnji točki dokazali, da imajo red potence števila 2. Zopet smo torej našli nek i in j, da je $red(x) = 2^i$ in $red(y) = 2^j$, kar pa po prejšnjem premisleku že pomeni, da je red g potenca števila 2.
- Vsi elementi g_i so različni od c in d. Ker se razlikujejo tudi od a, je element g torej enak $g = ababab \dots ab$, torej $g = (ab)^k$. Ker za ab že vemo, da je reda $16 = 2^4$, je $g^{16} = (ab)^{16 \cdot k} = 1^k = 1$. Seveda bi zadnjo točko lahko pokazali tudi podobno kot prejšnjo, tako da bi pokazali, da v x in y mora nastopati nek c, nato pa bi s sklicem na prejšnji dokaz našli red elementa k, v vsakem primeru pa bi nas to privedlo do konca dokaza.

□

V zadnjih treh točkah dokaza je jasno razvidno, zakaj je definicija avtomorfizma d takšna, da je njegovo zoženje na eno od poddreves kar identiteta. Ta lastnost

je namreč ključnega pomena, ker zagotovi končen red elementu ad, iz tega pa sledijo tudi končni redi ab in ac. Če povzamemo, smo pokazali, da ima grupa Γ tri pomembne lastnosti. Je neskončna, končnogenerirana in periodična, kar nam odgovarja na začetno vprašanje. Ali je vsaka končnogenerirana periodična grupa končna? Ne. Žal pa smo v zadnjem dokazu ob uporabi indukcijske predpostavke velikokrat naleteli na točko, kjer se je red elementa povečal za faktor 2. Tako nam ne preostane veliko upanja, da bi naša grupa odgovarjala tudi na drugo Burnsideovo vprašanje, ki se nanaša na periodične grupe z omejenim eksponentom. Vse upe dokončno poruši tudi izrek, ki pove, da za vsako naravno število n obstaja $g \in \Gamma$, za katerega velja $g^{2^n} \neq 1$, kar že pomeni, da je red elementa večji od 2^n (da ne more biti manjši, vemo, ker je Γ 2-grupa iz $g^{2^{n-i}} = 1$ za $i > 1$ pa sledi $g^{2^n} = g^{2^{n-i} \cdot 2^i} = 1$, kar vodi v protislovje). Dokaz tega izreka je še precej zahtevnejši od zgornjega, med drugim se nahaja v [1]. Čeprav smo z grupo Γ odgovorili samo na eno od dveh vprašanj, pa to ni samo pomankljivost. S tem smo namreč pokazali, da sta vprašanji dejansko dve, saj obstaja neskončna končnogenerirana periodična grupa, ki nima omejenega eksponenta (če takšna grupa ne bi obstajala, torej če bi iz končnogeneriranosti, neskončnosti in periodičnosti že sledilo, da ima grupa tudi omejeni eksponent, bi bili dve vprašanji na začetku povsem brez pomena, ker bi v vsakem primeru imeli isti odgovor).

6.5. **Podgrupe Γ.** Grigorčukova grupa ima poleg zgornje še mnogo zanimivih in pomembnih lastnosti, za razumevanje katerih je potrebno poznavanje kar nekaj definicij. Da ne odtavamo predaleč, si raje oglejmo še nekaj enostavnejših (a ne trivialnih) lastnosti grupe. Pred analizo treh njenih podgrup najprej osvežimo spomin na diedrske grupe. Diedrska grupa D_n je grupa vseh simetrij pravilnega n-kotnika. Ponavadi si predstavljamo, da jo generirata ena rotacija r (ki je reda n) in zrcaljenje f prek ene od diagonal (reda 2). Da n-kotnik zasučemo v drugo smer (torej da nanj delujemo z rotacijo), moramo lik najprej prezrcaliti, ga nato obrniti z r in prezrcaliti, razmislek, ki nam da enakost $frf^{-1} = frf = r^{-1}$. Naštete lastnosti so že dovolj za strogo definicijo diedrske grupe kot grupe, generirane z r in f, za katera velja $r^n = f^2 = 1$ in $frf = r^{-1}$, kar lahko zapišemo krajše.

Definicija 6.15. Diedrska grupa D_n *je grupa* $\langle r, f | r^n = f^2 = 1, frf = r^{-1} \rangle$.

Preden lahko v grupi Γ iščemo kakšne zanimive diedrske grupe, naletimo na težavo, saj bi, če bi iskali elementa r in f, morali najti en element reda n, v Γ pa večinoma poznamo elemente reda 2. Pomagamo si lahko z ekvivalentno definicijo diedrskih grup.

Izrek 6.16. *Diedrsko grupo D_n lahko predstavimo tudi kot*

$$D_n = \langle x, y | x^2 = y^2 = (xy)^n = 1 \rangle.$$

Vidimo, da je ta definicija diedrske grupe bolj primerna za naše razmere, saj bomo veliko hitreje našli dva elementa, katerih produkt je višjega reda, kot da bi element višjega reda iskali brez pomoči.

Dokaz. Če v D_n najdemo elementa, ki zadoščata zahtevam iz izreka, bomo očitno pokazali, da je grupa $G_n = \langle x, y | x^2 = y^2 = (xy)^n = 1 \rangle$ izomorfna podgrupi v D_n, kar bomo površno označili kar kot $G_n < D_n$. Če potem tudi v G_n najdemo elementa, ki zadoščata lastnostim iz definicije diedrske grupe, bomo pokazali še, da je D_n izomorfna podgrupi v G_n in s tem pokazali tudi izrek.

Ko v D_n iščemo element reda 2, se nam takoj ponudi kar generator f. Vzemimo torej $x = f$. Sedaj iščemo še y, da se bosta x in y zmnožila v element reda n. Kot element reda n se nam ponuja kar r, iz česar dobimo enačbo $fy = r$. Enačbo z leve pomnožimo z elementom f, kar nam da $y = fr$. Potem očitno velja $(xy)^n = (ffr)^n = r^n = 1$ Vidimo, da je grupa $\langle f, fr\rangle$ kar enaka grupi G_n, torej smo pokazali $G_n < D_n$
Razmislek v drugo smer bo sedaj še lažji, saj že vemo, katere elemente iskati. Očitno bomo za f vzeli generator x, več dela pa ne bomo imeli niti z drugim generatorjem. Element, ki ima v G_n red n, je namreč (po definiciji) kar xy. Če označimo $xy = r$, moramo preveriti še enakost $frf = r^{-1}$ oziroma $frfr = 1$. Ta velja, saj je $frfr = x(xy)x(xy) = (xx)y(xx)y = yy = 1$. Zaključimo lahko, da mora veljati $D_n < G_n$, kar dokazuje tudi naš dokaz, saj velja $D_n \cong G_n$. □

Oboroženi s kar dvema definicijama diedrske grupe lahko te sedaj poiščemo še v Γ.

Trditev 6.17. *Generatorji b, c in d skupaj z a generirajo diedrske grupe različnih moči, in sicer*

(1) $\langle a, d\rangle = D_4$,
(2) $\langle a, c\rangle = D_8$,
(3) $\langle a, d\rangle = D_{16}$.

Dokaz. Dokaz trditve je samo pregled že opravljenega dela. Vemo namreč že (trditev 6.3 in 6.6), da je $a^2 = b^2 = c^2 = d^2 = 1$, hkrati pa smo na začetku dokaza 6.14 tudi enakosti:

(1) $(ad)^4 = 1$, kar dokazuje $\langle a, d\rangle = D_4$,
(2) $(ac)^8 = 1$, kar dokazuje $\langle a, c\rangle = D_8$,
(3) $(ab)^{16} = 1$, kar dokazuje$\langle a, d\rangle = D_{16}$.

Dokaz torej sploh ni potreben, saj je delo že opravljeno. □

Še ena zanimiva podgrupa v Γ, vredna pogleda, je njen center. Ne, ker bi imela zanimivo notranjo strukturo, ampak ker je ni oziroma je trivialna.

Trditev 6.18. *Center grupe Γ je trivialen.*

Dokaz. Spomnimo se, da je center grupe množica tistih elementov grupe, ki komutirajo z vsemi ostalimi elementi. Torej $Z(\Gamma) = \{z \in \Gamma : \forall g \in \Gamma : zg = gz\}$. Vemo tudi, da elementa z in g komutirata natanko tedaj, ko velja $zgz^{-1} = g$ oziroma $[z, g] = zgz^{-1}g^{-1} = 1$. Vzemimo sedaj poljuben element $z \in \Gamma$.
Najprej poglejmo primer, ko z ni element $St_\Gamma(1)$. Tedaj je element $za = h$, ki zgornji vozlišči zamenja enkrat več kot z in na njiju torej deluje kot identiteta, element $St_\Gamma(1)$. Element z torej lahko napišemo kot ha za nek $h \in St_\Gamma(1)$, h pa lahko kot ponavadi predstavimo z njegovim delovanjem na levo in desno poddrevo, torej kot (h_0, h_1). Poglejmo sedaj, če z komutira z elementom d. Avtomorfizem $zdz^{-1} = hadah^{-1}$ je očitno element $St_\Gamma(1)$ (ker je produkt h, ada in h^{-1}, ti pa vsi ležijo v $St_\Gamma(1)$), zato na njem lahko uporabimo izomorfizem ψ. Dobimo

$$\psi(zdz^{-1}) = \psi(hadah^{-1}) = \psi(h)\psi(ada)\psi(h^{-1}) =$$
$$= (h_0, h_1)(b, 1)(h_0^{-1}, h_1^{-1}) = (h_0 b h_0^{-1}, h_1 h_1^{-1}) = (h_0 b h_0^{-1}, 1).$$

Ker se $\psi(zdz^{-1}) = (h_0 b h_0^{-1}, 1)$ razlikuje od $\psi(d) = (1, b)$ in je ψ (kot preslikava iz $St_{G^{(2)}}(1)$) bijekcija, zaključimo, da elementa z in d ne komutirata, kar pomeni

$z \notin Z(\Gamma)$ in posledično $Z(\Gamma) < St_\Gamma(1)$.
Primera $z \in St_\Gamma(1)$ se bomo spet lotili z indukcijo po dolžini okrajšane besede, ki predstavlja z. Naj bo torej $z_1 z_2 \dots z_n$ okrajšana beseda, ki predstavlja z.
Če je n enak 1, je $z \in \{b, c, d\}$, iz trditve 6.5 pa vemo, da ti trije elementi ne komutirajo z elementom a, zato niso v centru Γ. Besed dolžine 2 v $St_\Gamma(1)$ ni, besede dolžine 3 pa so aba, aca in ada, ki očitno ne komutirajo z a.
Predpostavimo sedaj, da trditev velja za vse z, ki jih predstavlja beseda dolžine, manjše od n. Ker vemo, da z leži v $St_\Gamma(1)$, vemo, da je število ponovitev elementa a v besedi $z_1 z_2 \dots z_n$ sodo. Zato lahko, podobno kot v dokazu izreka 6.14, besedo z preasociiramo tako, da vsakemu drugemu od a različnemu elementu dodamo njegov levi in desni a. Beseda, ki predstavlja z, je potem oblike $(ax_1a)x_2(ax_3a)\dots$ ali $y_1(ay_2a)y_3\dots$, v vsakem primeru pa vidimo, da je $\psi(z) = (z_0, z_1)$, kjer sta z_0 in z_1 besedi dolžine največ $\frac{n+1}{2}$. Ker lahko predpostavimo $n > 3$ in torej $\frac{n+1}{2} < n$, na z_0 in z_1 uporabimo indukcijsko predpostavko. Obstaja torej nek g_0, za katerega velja $z_0 g_0 \neq g_0 z_0$. Obstaja sicer tudi g_1', za katerega je $z_1 g_1' \neq g_1' z$, a element (g_0, g_1') mogoče sploh ni v Γ (vemo, da $\psi|_\Gamma$ ni bijekcija), a elementa g_1', ki ne komutira z z_1, dejansko ne potrebujemo. Potrebujemo le še nek element g_1, da bo (g_0, g_1) sploh slika nekega elementa iz $St_\Gamma(1)$. Ker je po trditvi 6.11 preslikava Φ_0 (komponenta izomorfizma ψ) surjektivna, vemo, da obstajata nek avtomorfizem g_1 iz $St_\Gamma(1)$ in g iz Γ, da je $\psi(g) = (g_0, g_1)$. Hkrati velja tudi:

$$\psi(gz) = \psi(g)\psi(z) = (g_0, g_1)(z_0, z_1) =$$
$$= (g_0 z_0, g_1 z_1) \neq (z_0 g_0, z_1 g_1) = \psi(zg).$$

Bijektivnost preslikave ψ je dovolj, da zaključimo, da z ni element centra Γ in da je center zato trivialen. □

6.6. **Druge zanimive lastnosti Γ.** Grupa Γ je odgovor na (ob času konstrukcije) 78 let staro Burnsideovo vprašanje, a to še zdaleč ni vse. Ima še mnogo drugih pomembnih lastnosti, med katerimi omenimo samo dve.

6.6.1. *Končna prezentabilnost.* Iz poglavja o diedrskih grupah se spomnimo, da smo lahko grupo D_n predstavili tako, da smo našteli njene generatorje in to, kako se ti generatorji množijo med sabo. Za grupo, ki jo lahko predstavimo s končno mnogo generatorji in končno mnogo relacijami med njimi, rečemo, da je *končno prezentabilna*. Bolj natančno je končno prezentabilna vsaka grupa, ki je izomorfna nekemu kvocientu F/R proste grupe F nad končno množico, kjer je R podgrupa edinka grupe F, ki je kot podgrupa edinka v F generirana s končno mnogo elementi.

Primer 3. (1) *Grupa $\mathbb{Z}$ je končno prezentabilna, saj je pravzaprav tudi prosta grupa nad množico $S = \{1\}$.*
(2) *Grupa $\mathbb{Z}_n$ je končno prezentabilna za vsak $n \in \mathbb{N}$, saj je kvocient grupe $\mathbb{Z}$ ($\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$).*
(3) *Grupa D_n je končno prezentabilna za vsak $n \in \mathbb{N}$. Je namreč enaka kvocientu F/R, kjer je F prosta grupa na dveh generatorjih in R grupa, generirana z besedami r^2, f^n in $frfr$. Ko namreč naredimo kvocient F/R, bomo generatorjema rR in fR dali natanko tiste lastnosti, ki jih želimo. Veljalo bo $(rR)(rR) = r^2R = 1R$, kjer je $1R$ seveda enota v F/R, podobno pa bomo v grupi F/R dobili tudi lastnosti $f^n = 1$ in $frf = r^{-}1$, kar je ekvivalentno $frfr = 1$.*

Opomba 6.19. *Dejali smo, da je R podgrupa, ki je kot podgrupa edinka generirana s končno mnogo elementi. To ne pomeni, da je R grupa, ki je generirana s končno mnogo elementi in je poleg tega še edinka, ampak da je R najmanjša podgrupa edinka grupe F, ki vsebuje neko končno generatorsko množico. Razlika med dvema je navidez majhna, a zelo pomembna, saj vsaj v enostavnih grupah (tam pravih netrivialnih podgrup edink sploh ni) lahko obstajajo podgrupe, ki so generirane same s sabo, a je podgrupa, ki je kot podgrupa edinka generirana z njimi, nujno kar celotna enostavna grupa.*

Primerov končno prezentabilnih grup je v matematiki na pretek, zato bi nas lahko zaneslo, da bi grupo Γ prav tako poskušali predstaviti z neko množico relacij med generatorji. Poznamo namreč relacije $x^2 = 1$ za $x \in \{a, b, c, d\}$, $bc = cb = d$, $cd = dc = b$ in $bd = db = c$, grupa pa je tudi, kot vse končno prezentabilne, končnogenerirana. Žal (ali pa na srečo) je Γ ravno grupa, ki dokazuje, da vsaka končnogenerirana grupa še ni končno prezentabilna, saj ni izomorfna nobenemu kvocientu F/R, kjer je F prosta grupa nad končno množico in R podgrupa F, ki je kot podgrupa edinka v F generirana s končno mnogo elementi. Razmeroma tehničen dokaz te lastnosti se med drugim nahaja v [1].

6.6.2. *Rast.* Še ena pomembna lastnost Γ se dotika njene "rasti". *Rast* končnogenerirane grupe G je funkcija naravnih števil, ki za vsako naravno število n pove, koliko elementov grupe Γ se da predstaviti z besedo dolžine n. Zanima nas predvsem to, kako hitro ta funkcija zraste preko vsakih mej, ne pa njen natančen potek, zato za ekvivalentni proglasimo poljubni funkciji f in g, za kateri obstaja konstanta C, da je $f(n/C) < g(n) < f(Cn)$ (hitro lahko ugotovimo, da sta ekvivalentna poljubna polinoma iste stopnje). Sedaj nas ne zanima več točen potek funkcije rasti, vendar samo še to, v kateri ekvivalenčni razred pade, torej ali je linearna, kvadratična, logaritemska ali kaj četrtega. Takšna postavitev vprašanja je smiselna predvsem zato, ker funkcija rasti, ki je odvisna tudi od začetne izbire generatorjev, ob poljubni izbiri generatorjev spada v isti ekvivalenčni razred.
Nekaj ekvivalenčnih razredov poznamo zelo dobro. Veliko znamo povedati o poljubnem polinomu, vemo pa tudi, da je funkcija, ki je hitrejša od vsakega polinoma, eksponentna, o vrzeli med funkcijami polinomske rasti in tistimi eksponentne rasti pa vemo tako malo, da je bilo vprašanje, če obstaja kakšna grupa, katere rast spada vanjo, dolgo časa neodgovorjeno. Nanj odgovarja Grigorčukova grupa Γ, saj zanjo velja, da je funkcije

$$f(n) = |\{g \in \Gamma : g = g_1 g_2 \cdots g_m; m \leq n, g_i \in \{a, b, c, d\}\}|$$

hitrejša od polinomske (za vsak polinom p gre kvocient $\frac{p(n)}{f(n)}$ proti 0, ko gre n preko vseh mej), hkrati pa je počasnejša od vseh eksponentnih funkcij (za vsak $a > 1$ gre $\frac{f(n)}{a^n}$ proti 0, ko gre n preko vseh mej). Za podrobnejšo obravnavo te lastnosti je možen vir tudi [1].

7. Zaključek

Pri dokazovanju težkih in zapletenih izrekov je človeška intuicija pogosto zadnja rešilna bilka za matematika v stiski, dobro razvita intuicija pa je natanko tisto, kar odlikuje najboljše raziskovalce. Verjetno so tudi zato težki problemi pogosto tisti, pri katerih intuicija na začetku odpove. Takšen je tudi Burnsideov problem, pri katerem je začetno vprašanje tako, da odgovor nanj izgleda kot jasen *da*. Grigorčukova grupa

nam kaže, da je torej naš občutek, če mu pustimo preveč prosto pot, pogosto mnogo preveč zaletav. Tako bi ob hitrem pogledu verjetno radi vzkliknili, da je vsaka končnogenerirana grupa tudi končno prezentabilna in da funkcij, katerih hitrost ni ne polinomska ne eksponentna, ampak je nekaj vmes, preprosto ne more biti.
Pesimist bi ob pogledu na grupo Γ torej grupo opisal kot tisto črno ovco v družini, tisto "grdo"grupo, ki se ne obnaša tako, kot bi se morala, a tak pogled je vse preveč kratkoviden. Grupa Γ je namreč ena tistih grup, ki nam kažejo, da naše raziskovanje grup ne sme biti omejeno samo z našo intuicijo. Je grupa, ki kaže, da je teorija grup mnogo kompleksnejša in zanimivejša, kot si jo sprva predstavljamo. Je grupa, ki dokazuje, da je matematika manj preprosta, a zato toliko bolj zanimiva, kot se zdi na prvi pogled.

Literatura

[1] P. de la Harpe, *Topics in Geometric Group Theory*, Chicago, The University of Chicago Press 2000, 211–259.

[2] C. Velkovrh, *Nekaj navodil avtorjem za pripravo rokopisa*, Obzornik mat. fiz. **21** (1974) 62–64.

[3] R. I. Grigorčuk, *On Burnside's problem on periodic groups*, Funktsional. Anal. i Prilozhen., **14(1)** (1980) 53–54.