UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO
Pedagoška matematika

Špela Povše

DELOVANJA PROSTIH GRUP NA DREVESA

Magistrsko delo

Mentor: doc. dr. Aleš Vavpetič

Ljubljana, 2015

Podpisana Špela Povše izjavljam:

- da sem magistrsko delo z naslovom *Delovanja prostih grup na drevesa* izdelala samostojno pod mentorstvom doc. dr. Aleša Vavpetiča in
- da Fakulteti za matematiko in fiziko Univerze v Ljubljani dovoljujem objavo elektronske oblike svojega dela na spletnih straneh.

Ljubljana, 20. 3. 2015 Podpis: .....

Zahvala

Zahvaljujem se mentorju doc. dr. Alešu Vavpetiču za vso pomoč in vse nasvete pri pisanju magistrskega dela. Posebna zahvala gre staršema Romani in Binetu, ki sta me podpirala in mi stala ob strani skozi celotno šolanje. Zahvaljujem se tudi Gregi, ki me je bodril in spodbujal, kadarkoli sem to potrebovala. Hvala pa tudi Sandi in Lojzetu za odlične študijske pogoje.

Kazalo

Program dela

V magistrskem delu obravnavajte delovanja grup na grafe. Pokažite, da je grupa prosta natanko tedaj, ko deluje prosto na drevo.

Osnovna literatura:
John Meier, *Groups, graphs and Trees. An introduction to the geometry of infinite groups*, London Mathematical Society Student Texts 73, Cambridge University Press, Cambridge, 2008.

Ljubljana, 2015 doc. dr. Aleš Vavpetič

Povzetek

Tekom magistrskega dela Delovanja prostih grup na drevesa se prikaže moč prepletanja algebraičnih in geometričnih pristopov v teoriji grup. Ključen korak od grup do geometrije naredimo z vpeljavo Cayleyjevih grafov, s pomočjo katerih nazorneje pojasnimo koncept abstraktnih grup. Z delovanjem grup na matematični objekt ponudimo še en geometrični pogled na grupe, saj lahko preko delovanja grupe na nek objekt ustvarimo posplošitev dane grupe na grupo simetrij danega objekta. Proste grupe, ki so v osnovi čisto algebraičen pojem, lahko geometrično opredelimo s pomočjo delovanj na drevesa. Geometrijska karakterizacija prostih grup pravi, da je grupa prosta natanko tedaj, ko omogoča prosto delovanje na drevo. Ta karakterizacija nas pripelje do elegantnega dokaza Nielsen-Schreierjevega izreka, ki trdi, da so podgrupe prostih grup proste.

Abstract

The work Actions of free groups on trees shows the power of interlacing algebraic and geometric approaches in group theory. An essential step from groups to geometry is made by the definition of Cayley graphs, which offers the demonstration of abstract groups. Another geometric perspective of groups is offered by actions of groups on a mathematical object. Action of a group on an object creates a generalization of the group to the symmetry group of a given object. Free groups, a purely algebraic concept, can be characterised via actions on trees. Geometric characterization of free groups says that the group is free if and only if it acts freely on a tree. This leads to an elegant proof of the purely algebraic fact that subgroups of free groups are free. The last fact is called the Nielsen-Schreier theorem.

Math. Subj. Class. (2010): 20E05, 20E08, 20F65, 05E18

Ključne besede: grupa, delovanje grupe, množica generatorjev, Cayleyjev graf, prosta grupa, drevo, delovanje proste grupe

Keywords: group, group action, generating set, Cayley graph, free group, tree, free group action

1 Uvod

Vsebina, ki je obravnavana v magistrskem delu, spada v geometrično teorijo grup. To polje raziskuje interakcije med algebraičnimi in geometričnimi lastnostmi grup. Obenem je to zanimiva teorija, ki kombinira aspekte različnih matematičnih polj in igra pomembno vlogo tudi pri reševanju problemov v bolj klasičnih vejah matematike, kot je teorija grup. Geometrična teorija grup se med drugim ukvarja tudi z vprašanjem, ali lahko na grupe gledamo kot na geometrične objekte in kako so med seboj povezane geometrične in algebraične lastnosti grup.

Praviloma so invariante grup asociirane z geometričnimi objekti, kot je na primer grupa izometrij. Eden osrednjih vpogledov, ki vodi do geometrične teorije grup, je ta, da lahko zgornji proces asociiranja grup z geometričnimi objekti do neke mere tudi obrnemo. Želimo si povezati nek geometrični objekt z grupo, ki jo obravnavamo. Ta povezava je lahko posledica neke umetne, abstraktne konstrukcije ali pa zelo konkretnega prostora, kot je na primer Evklidska ravnina. To storimo tako, da poiščemo geometrične invariante in jih apliciramo na geometrične objekte. To nam omogoči, da prevedemo geometrične izraze, kot so ukrivljenost in volumen, v teorijo grup. Da bi pridobili dobre invariante, moramo večkrat omejiti svojo pozornost na končno generirane grupe in vzeti geometrične invariante iz geometrije v velikem merilu. Na koncu primerjamo obnašanje teh geometričnih invariant grup z obnašanjem v algebraičnem smislu in premislimo, kaj vse lahko pridobimo s to simbiozo med geometrijo in algebro.

Eden ključnih zgledov, kako pridobiti geometrijski objekt iz grupe, je preučevanje t.i. *Cayleyjevih grafov* glede na izbrano množico generatorjev skupaj z ustrezno besedno metriko.

Geometrična teorija grup ima številne povezave s problemi v algebri. Oglejmo si jih le nekaj: proste grupe, ki so v osnovi čisto algebraičen pojem, lahko karakteriziramo geometrično preko njihovega delovanja na drevesa. To vodi tudi do elegantnega dokaza algebraičnega dejstva, da so podgrupe prostih grup proste. S pomočjo geometrične teorije grup lahko prepoznamo, da so določene grupe končno generirane, to lahko storimo tako, da poiščemo dobro delovanje grupe na ustreznem prostoru. Med drugim pa si lahko z geometrično teorijo grup pomagamo tudi pri prepoznavanju, da so določene grupe matrik proste grupe. Obstaja namreč geometrični kriterij, t.i. Ping-pong lema, ki nam omogoči, da preko ustreznega delovanja grupe razberemo, ali je dana grupa prosta.

Ker so v geometrični teoriji grup ključni deli grupe, si bomo v magistrskem delu najprej osvežili spomin s pregledom nekaterih konceptov in primerov iz teorije grup. Nato bomo nadaljevali s predstavitvijo osrednjih kombinatoričnih objektov v geometrični teoriji grup, s Cayleyjevimi grafi. Sledi raziskovanje geometrične karakterizacije prostih grup, kjer se nam bo prvič pokazal učinek geometrične teorije grup.

Osnovna literatura za magistrsko delo sestoji iz knjig [9] in [10].

2 Kratek uvod v teorijo grup

V tem poglavju bomo strnili osnovne pojme teorije grup, s katerimi se bomo srečali v magistrskem delu, le-ti so povzeti iz knjig [2], [9] ter [12].

2.1 Aksiomatični opis grup

Definicija 2.1. *Grupa* je množica G opremljena z binarno operacijo $\cdot : G \times G \to G$. Po tej operaciji pripada vsakemu urejenemu paru $g_1, g_2 \in G$ natanko določen element v G. Ta element imenujemo kompozitum ali produkt in ga pišemo kot $g_1 \cdot g_2$. Pri tem morajo biti izpolnjeni naslednji pogoji:

- *Asociativnostni zakon*: za poljubne elemente $g_1, g_2, g_3 \in G$ velja

$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3.$$

- *Obstoj nevtralnega elementa*: za binarno operacijo $\cdot$ obstaja nevtralni element $e \in G$, da za vsak $g \in G$ velja

$$e \cdot g = g \cdot e = g.$$

- *Obstoj inverznega elementa*: za vsak $g \in G$ obstaja inverzni element g^{-1} glede na binarno operacijo $\cdot$ in velja

$$g \cdot g^{-1} = g^{-1} \cdot g = e.$$

Včasih zapišemo $g \cdot h$ krajše kot gh.

Grupa G je *Abelova*, če je operacija v grupi komutativna, če je torej $g_1 \cdot g_2 = g_2 \cdot g_1$ za vse $g_1, g_2 \in G$.

Grupa ima lahko končno ali neskončno število elementov. V prvem primeru jo imenujemo *končna grupa*, številu elementov v končni grupi pa rečemo *moč grupe*.

Definicija 2.2. Naj bo G grupa. Neprazna podmnožica H grupe G je *podgrupa*, če je za isto binarno operacijo oziroma za zožitev te operacije na $H \times H$ tudi sama grupa. To označimo z oznako $H \leq G$.

Primer 2.3. Oglejmo si nekaj osnovnih primerov grup in podgrup:

- *Trivialna grupa* je grupa, sestavljena iz enega samega elementa e in kompozituma $(e, e) \mapsto e$. Vsaka grupa vsebuje trivialno grupo, dano z nevtralnim elementom grupe, kot svojo podgrupo.

- Množice $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ so grupe za seštevanje. Velja tudi, da je $\mathbb{Z}$ podgrupa grupe $\mathbb{Q}$, $\mathbb{Q}$ pa je podgrupa grupe $\mathbb{R}$. Te množice niso grupe za množenje, so pa to naslednje grupe: $\mathbb{Z}^* = \{1, -1\}$, $\mathbb{Q}^* = \mathbb{Q} \backslash \{0\}$, $\mathbb{R}^* = \mathbb{R} \backslash \{0\}$.

Zgoraj smo aksiomatično opisali grupe, sedaj pa potrebujemo še morfizme, da bomo lahko med seboj povezali grupe in različne matematične objekte. Podobno kot v drugih matematičnih teorijah naj bi tudi tu morfizmi ohranjali strukturo objekta, ki ga obravnavamo. Prav tako pa smatramo dva objekta za enaka, če imata enako strukturo.

Definicija 2.4. Naj bosta G in H grupi.

- *Homomorfizem* iz grupe G v grupo H je preslikava $\varphi\colon G \to H$, za katero velja

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \quad \forall g_1, g_2 \in G.$$

  Opazimo, da je v enačbi $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ operacija $g_1 g_2$ na levi strani enačbe operacija v grupi G, medtem ko je operacija $\varphi(g_1)\varphi(g_2)$ na desni strani enačbe operacija v grupi H.

- Homomorfizem grup $\varphi\colon G \to H$ je *izomorfizem grup*, če obstaja tak homomorfizem grup $\psi\colon H \to G$, da velja $\varphi \circ \psi = id_H$ in $\psi \circ \varphi = id_G$. Če med G in H obstaja izomorfizem grup, potem sta si G in H izomorfni grupi. To označimo z $G \cong H$. Algebraiki v osnovi smatrajo izomorfne si grupe kot enake in pogosto ne razlikujejo med njimi.

Lema 2.5. *Če je $\varphi\colon G \to H$ homomorfizem grup G in H, potem velja:*

1. *Vsak homomorfizem grup ohranja nevtralni element, torej velja $\varphi(e) = e$, kjer je e nevtralni element posamezne grupe.*
2. *Za vsak $g \in G$ je $\varphi(g^{-1}) = \varphi(g)^{-1}$.*

Dokaz:

1. Ker je φ homomorfizem grup, je $\varphi(e) = \varphi(e^2) = \varphi(e)^2$. Iz zgornjega sledi, da velja $\varphi(e) = e$.
2. Iz prve točke naše leme in dejstva, da je φ homomorfizem grup, sledi, da je $e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$. Torej velja enakost $\varphi(g^{-1}) = \varphi(g)^{-1}$.

■

Primer 2.6. Oglejmo si nekaj primerov homomorfizmov grup:

- Če je H podgrupa grupe G, potem je vložitev $H \hookrightarrow G$ homomorfizem grup.
- Naj bo $n \in \mathbb{Z}$. Potem je

$$\begin{aligned} &\mathbb{Z} \to \mathbb{Z}, \\ &x \mapsto n \cdot x, \end{aligned}$$

homomorfizem grup. Toda prištevanje neničelnega števila n k $x \in \mathbb{Z}$,

$$\begin{aligned} &\mathbb{Z} \to \mathbb{Z}, \\ &x \mapsto n + x, \end{aligned}$$

pa ni homomorfizem grup, ker ta preslikava ne ohranja nevtralnega elementa.

- Eksponentna preslikava $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ je homomorfizem med grupo za seštevanje $\mathbb{R}$ in grupo za množenje $\mathbb{R}_{>0}$:

$$\exp(a + b) = \exp(a) \cdot \exp(b).$$

Velja še več, omenjena preslikava je izomorfizem. Inverzni homomorfizem je logaritemska preslikava.

Definicija 2.7. Naj bo $\varphi\colon G \to H$ homomorfizem grup. Podgrupo grupe G

$$\ker \varphi := \{g \in G \mid \varphi(g) = e\}$$

imenujemo *jedro* homomorfizma φ. Podgrupi grupe H

$$\operatorname{im} \varphi := \{\varphi(g) \mid g \in G\}$$

pa pravimo *slika* homomorfizma φ.

Opomba 2.8. Oglejmo si pojem izomorfizma preko jedra in slike homomorfizma. Naj bo $\varphi\colon G \to H$ homomorfizem grup G in H.

1. Homomorfizem grup φ je injektiven, če in samo če je jedro tega homomorfizma trivialna podgrupa grupe G.

2. Homomorfizem grup φ je izomorfizem, če in samo če je $\ker \varphi$ trivialna podgrupa grupe G in $\operatorname{im} \varphi = H$.

Dokaz zapisanega v tej opombi lahko zasledimo v knjigi [12, str. 50,51].

2.2 Zgledi zanimivih grup

Zgled 2.9. *Ciklična grupa* je grupa, generirana z enim samim generatorjem. To pomeni, da je grupa G *ciklična*, če obstaja tak element grupe $a \in G$, da velja $G = \{..., a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, ...\}$. V tem primeru uporabimo zapis $G = \langle a \rangle$.

Ciklične grupe delimo v dve skupini:

1. Ciklične grupe, kjer so si vse potence elementa $a \in G$ med seboj različne. To pomeni, da je $G = \langle a \rangle = \{..., a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, ...\} = \{a^n \mid n \in \mathbb{Z}\}$ neskončna grupa.

2. Ciklične grupe, v katerih obstajata števili $i > j \in \mathbb{N}$ tako, da velja $a^i = a^j$. To pomeni, da obstaja tako naravno število n, da je $a^n = e$. Najmanjšemu eksponentu $n \in \mathbb{N}$, za katerega velja slednja enakost, pravimo *red elementa a*.

Zgled 2.10. Pravilni n-kotnik ima $2n$ simetrij, od tega ima n rotacijskih in n zrcalnih simetrij. Pripadajoče rotacije in zrcaljenja tvorijo *diedrsko grupo* D_n. Diedrska grupa ima torej elemente $R_0, ..., R_{n-1}$, ki predstavljajo rotacije pravilnega n-kotnika in $S_0, ..., S_{n-1}$, ki so zrcaljenja preko simetrijskih osi pravilnega n-kotnika. Operacija v diedrski grupi pa je kompozitum zrcaljenj in rotacij. Za zgornje elemente veljajo naslednje enakosti:

$$\begin{aligned} R_i R_j &= R_{i+j}, \\ R_i S_j &= S_{i+j}, \\ S_i R_j &= S_{i-j}, \\ S_i S_j &= R_{i-j}. \end{aligned}$$

V splošnem se izkaže, da je diedrska grupa generirana z 2 elementoma r in s, kjer je r rotacija okoli središča n-kotnika za kot $\frac{2\pi}{n}$, s pa je zrcaljenje preko neke simetrijske osi v danem n-kotniku. To diedrsko grupo lahko zapišemo kot

$$D_n = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$$

ali kot

$$D_n = \langle r^\alpha s^\beta \mid \alpha \in \{0, 1, ..., n-1\},\ \beta \in \{0, 1\} \rangle.$$

Iz tega zapisa je razvidno, da je red elementa r enak n in red elementa s enak 2 ter da je moč diedrske grupe D_n enaka $2n$.

Oglejmo si zgled grupe vseh simetrij enakostraničnega trikotnika. Zanima nas, kakšna je diedrska grupa D_3. Ta grupa je generirana z 2 elementoma: z elementom a, ki je rotacija okrog središča trikotnika za kot $\frac{2\pi}{3}$, in b, ki je zrcaljenje preko simetrale ene od stranic. Rotacija a je element reda 3, zrcaljenje b pa element reda 2. Diedrsko grupo D_3 lahko zapišemo kot množico s šestimi elementi:

$$D_3 = \{e, a, a^2, b, ab, a^2 b\}.$$

Zgled 2.11. Naj bo X množica. Potem množica vseh bijekcij tipa $X \to X$ tvori grupo za komponiranje preslikav. To grupo označimo s $\mathrm{Sym}(X)$ in ji pravimo *simetrična grupa* ali *grupa permutacij*. Zapišimo jo še simbolno:

$$\mathrm{Sym}(X) = \{f \colon X \to X \mid f \text{ bijekcija}\}.$$

Elementi grupe permutacij množice X se imenujejo *permutacije* in od tod grupi tudi ime. Z oznako S_n označimo simetrično grupo vseh permutacij množice $[n] = \{1, 2, ..., n\}$. Njena moč je enaka $n!$. Grupa permutacij S_n je nekomutativna, če je $n > 2$.

Zgled 2.12. Naj bo X metrični prostor. Množica vseh izometrij tipa $X \to X$, ki jo označimo z $\mathrm{Isom}(X)$, tvori grupo za komponiranje preslikav. Ta množica je hkrati tudi podgrupa simetrične grupe $\mathrm{Sym}(X)$.

Simetrijska grupa danega objekta je grupa vseh izometrij, pod katerim so te invariantne za kompozitum kot operacijo. Simetrijska grupa je podgrupa izometrijske grupe. Kot objekt večkrat nastopajo različne geometrijske oblike, kot so liki, slike, vzorci. Na ta način se diedrske grupe naravno pojavijo kot simetrijske grupe pravilnih večkotnikov.

Zgled 2.13. Naj bo G grupa. Potem z $\mathrm{Aut}(G)$ označimo množico vseh izomorfizmov grup tipa $G \to G$, čemur krajše rečemo avtomorfizem grupe G. Množica $\mathrm{Aut}(G)$ je grupa za komponiranje preslikav, poimenujemo pa jo *grupa avtomorfizmov grupe* G. Dokaz, da je množica vseh avtomorfizmov grupe G res grupa, si lahko ogledate v knjigi [12, str. 55].

3 Cayleyjevi izreki

To poglavje se začne z definicijo delovanja grupe na objekt in z osnovnim Cayleyjevim izrekom, nato se predstavi notacija, terminologija in podlaga za nadaljne delo, zaključi pa se s konstrukcijo in osnovnim raziskovanjem Cayleyjevih grafov.

3.1 Cayleyjev osnovni izrek

Pomemben vidik v magistrski nalogi je preučevanje grup preko delovanj, zato se na začetku tega razdelka spomnimo same definicije delovanja grupe na nek matematični objekt, nato pa nadaljujemo s Cayleyjevim osnovnim izrekom. Ta razdelek je povzet po knjigi [10], sama definicija delovanja grupe na matematični objekt pa je povzeta po knjigah [1] in [9].

Spomnimo se, da za objekt X v kategoriji Kat z $\mathrm{Aut}_{\mathrm{Kat}}(X)$ označimo množico vseh avtomorfizmov v kategoriji Kat objekta X ter da je to grupa za kompozitum v kategoriji Kat.

Definicija 3.1. Naj bo G grupa, Kat kategorija in X objekt v kategoriji Kat. *Delovanje grupe G na objekt X v kategoriji* Kat je homomorfizem grup $G \to \mathrm{Aut}_{\mathrm{Kat}}(X)$. Z drugimi besedami, delovanje grupe G na objekt X sestoji iz družine $(f_g)_{g\in G}$ avtomorfizmov objekta X, za katero velja

$$f_g \circ f_h = f_{gh},$$

za vsaka $g, h \in G$. Delovanje grupe G na objekt X označimo z $G \curvearrowright X$.

Opomba 3.2. Poskusimo malce bolje preučiti zgornjo definicijo:

- Vsaka grupa dovoli delovanje na poljuben objekt X v katerikoli kategoriji Kat, to delovanje poimenujemo *trivialno delovanje* in ga zapišemo kot:

$$\begin{aligned} G &\to \mathrm{Aut}_{\mathrm{Kat}}(X) \\ g &\mapsto \mathrm{id}_X\,. \end{aligned}$$

- Naj bo G grupa in X množica v kategoriji množic M. Če je $\varphi\colon G \to \mathrm{Aut}_M(X)$ delovanje grupe G na množico X preko bijekcij, potem za $g \in G$ in $x \in X$ uporabimo zapis

  $$g \cdot x := (\varphi(g))(x).$$

  V tem primeru lahko na homomorfizem φ gledamo tudi kot na preslikavo $G \times X \to X$. Takšen zapis v splošnem uporabimo, kadarkoli grupa G deluje na objekt v kategoriji, v kateri so morfizmi preslikave množic in je kompozitum morfizmov v bistvu le kompozitum preslikav.

Če povzamemo, delovanje grupe G na množico X je homomorfizem $\varphi : G \to \mathrm{Sym}(X)$ iz grupe G v grupo permutacij $\mathrm{Sym}(X)$. Za vsak $g \in G$ homomorfizem φ poda permutacijo $\varphi(g)$ elementov v množici X. Če sta $g, h \in G$, je permutacija $\varphi(gh)$ enaka kompozitumu $\varphi(g)\varphi(h)$, saj je φ homomorfizem. To si predstavljamo, kot da elementi grupe G permutirajo elemente v množici X na način, ki je združljiv z algebrsko strukturo grupe G.

Pogosto bomo naš okorni zapis $(\varphi(g))(x)$ poenostavili z $g(x)$ za sliko elementa $x \in X$ glede na permutacijo, ki ustreza elementu $g \in G$. Zahteva, da je φ homomorfizem, se nato preoblikuje v

$$gh(x) = g(h(x)).$$

Povzemimo drugi del zgornje opombe v definicijo delovanja grupe na množico.

Definicija 3.3. Naj bo G grupa in X množica. Delovanje grupe G na množico X je preslikava $\varphi\colon G \times X \to X$, za katero veljata naslednji pravili:

1. $\varphi(e, x) = x$ za vsak $x \in X$;
2. $\varphi(gh, x) = \varphi(g, \varphi(h, x))$ za vse $g, h \in G$ in $x \in X$.

V literaturi se pogosto namesto zapisa s φ uporablja krajši zapis s $\cdot$: $\varphi(g, x) = g \cdot x$.

Če grupa G deluje na množico X, lahko za vsak element $g \in G$ definiramo preslikavo $L_g : X \to X$ s predpisom $L_g(x) = g \cdot x$. Ker ima definirana preslikava inverzno preslikavo $L_{g^{-1}}$, je preslikava L_g bijekcija. Zato lahko na L_g gledamo kot na element grupe permutacij množice X, torej velja $L_g \in \mathrm{Sym}(X)$. Iz drugega pravila definicije 3.3 sledi, da velja enakost $L_{gh} = L_g \cdot L_h$. Torej je preslikava $g \mapsto \mathrm{Sym}(X)$, kjer je $g \in G$, homomorfizem iz grupe G v grupo permutacij $\mathrm{Sym}(X)$. Pripadajoči homomorfizem iz G v $\mathrm{Sym}(X)$ pogosto poimenujemo *reprezentacija grupe* G.

Opomba 3.4. Z besedno zvezo delovanje grupe se bomo nanašali na levo delovanje, kot je opisano zgoraj v definiciji. Pomembno je, da razlikujemo med levim in desnim delovanjem, saj niso vse grupe Abelove. Levo delovanje pa smo si izbrali, ker ustreza notaciji funkcij in ker je standardno v teoriji grup.

Opomba 3.5. Za trenutek se ustavimo še pri konvenciji. Če je X matematični objekt, na primer pravilni n-kotnik ali množica števil, potem z oznako $\mathrm{Sym}(X)$ označimo množico vseh bijekcij tipa $X \to X$, ki ohranijo omenjeno matematično strukturo X. Na primer, če je X množica, potem je $\mathrm{Sym}(X)$ preprosto grupa permutacij elementov množice X. Če pa je X pravilni n-kotnik, potem moramo biti pozorni tudi na njegove kote in dolžine, zato bo $\mathrm{Sym}(X)$ sestavljena iz rotacij in zrcaljenj, torej bo kar diedrska grupa D_n.

Grupa $\mathrm{Sym}(X)$ ima številne oznake in se v matematiki uporablja v različnih kontekstih. Če je G grupa, potem zbirko vseh njenih simetrij označimo z $\mathrm{Aut}(G)$,

grupo avtomorfizmov grupe G. Če se ukvarjamo z Evklidsko ravnino $\mathbb{R}^2$ in s funkcijami, ki ohranjajo razdaljo med točkami v ravnini, potem množico takšnih funkcij označimo z $\mathrm{Isom}(\mathbb{R}^2)$ in jo poimenujemo kot grupo izometrij ravnine. Koristno je, če uporabljamo posamezna imena za te grupe simetrij, saj že njihovo ime nakaže, katere matematične strukture se preko simetrij ohranijo.

Primer 3.6. Oglejmo si nekaj primerov delovanj grup na množico ali geometrijski objekt:

- Vsaka grupa G lahko deluje sama nase na več načinov. Najpogostejše je delovanje z levim množenjem, t.j. $g \cdot x = gx$ za vse $g, x \in G$ in delovanje s konjugiranjem, t.j. $g \cdot x = gxg^{-1}$.
- Ciklična grupa $\mathbb{Z}_n$ reda n, deluje na pravilni n-kotnik z rotacijami.
- Diedrska grupa D_n reda $2n$ prav tako deluje na pravilni n-kotnik, vendar tu elementi grupe rotirajo ali zrcalijo večkotnik.
- Simetrična grupa S_n in njene podgrupe naravno delujejo na množico $[n] = \{1, 2, ..., n\}$ tako, da permutirajo njene elemente.

Definicija 3.7. Delovanje grupe G na množico X je

- *tranzitivno*, če za poljubna elementa $x, y \in X$ obstaja tak element $g \in G$, da je $g \cdot x = y$;
- *zvesto*, če za poljubna različna si elementa $g, h \in G$ obstaja nek $x \in X$, da velja $g \cdot x \neq h \cdot x$. Z drugimi besedami, delovanje grupe G na množico X je zvesto, če je pripadajoči homomorfizem $\varphi \colon G \to \mathrm{Sym}(X)$ injektiven;
- *prosto*, če neenakost $g \cdot x \neq x$ velja za vse $g \in G \setminus \{e\}$ in vse $x \in X$. Z drugimi besedami, delovanje grupe G na množico X je prosto, če in samo če vsak netrivialen element grupe G deluje na množico X brez negibnih točk.

Primer 3.8. Diedrska grupa D_n je simetrijska grupa pravilnega n-kotnika. Kot taka permutira oglišča večkotnika, zato imamo homomorfizem iz grupe D_n v grupo permutacij oglišč S_n. Ker vsak element, ki ni identiteta, premakne vsaj $(n-2)$ oglišč pravilnega n-kotnika, je delovanje zvesto.

Opomba 3.9. Grupa G deluje zvesto na množico X natanko tedaj, ko ima homomorfizem $G \to \mathrm{Sym}(X)$ trivialno jedro. V tem primeru je G izomorfna svoji sliki v $\mathrm{Sym}(X)$. Ker je delovanje vsake grupe same nase z levim množenjem tranzitivno, prosto in zvesto, je vsaka grupa izomorfna neki grupi permutacij svojih elementov, kar v podobni luči spoznamo tudi preko Cayleyjevega izreka.

Grupe pogosto nastopajo kot simetrije številnih matematičnih objektov. V teh primerih lahko izluščimo lastnosti in razumevanje grupe direktno iz našega razumevanja objekta X. Dva primera takšnega razumevanja sta simetrična in diedrska grupa. Vendar ne smemo pozabiti, da so grupe abstraktni objekti, ki zadoščajo določenemu seznamu zahtev. Cayleyjev izrek nam pokaže, da je abstrakten pojem grupe in pojem grupe permutacij pravzaprav eno in isto.

Izrek 3.10 (Cayleyjev osnovni izrek)**.** *Vsako grupo lahko zvesto reprezentiramo kot grupo permutacij.*

Opomba 3.11. Zgornji izrek nam pove, da obstaja injektivni homomorfizem iz grupe G v simetrično grupo $\mathrm{Sym}(G)$. To pomeni, da lahko vsako grupo vložimo v grupo permutacij svojih elementov.

Dokaz: Objekti, ki jih G permutira, so elementi grupe G. V tem dokazu uporabimo oznako S_G za simetrično grupo $\mathrm{Sym}(G)$, saj želimo s tem poudariti, da G označuje le množico elementov grupe G in ne celotne grupe. Permutacija, pripadajoča elementu $g \in G$, je definirana z levim množenjem z g: $g \mapsto \pi_g \in S_G$, kjer je $\pi_g(h) = g \cdot h$ za vsak $h \in G$. To je permutacija elementov grupe G, saj če je $g \cdot h = g \cdot h'$, potem po pravilu krajšanja z leve sledi, da je $h = h'$. Označimo preslikavo, ki pošlje element g v permutacijo π_g, kar s $\pi \colon G \to S_G$.

Da bi dokazali, da je π res homomorfizem grup, moramo preveriti, da velja $\pi(gh) = \pi(g) \cdot \pi(h)$ oziroma pokazati, da velja $\pi_{gh} = \pi_g \cdot \pi_h$. To storimo tako, da ocenimo, kaj vsaka stran enakosti stori s poljubnim elementom grupe $x \in G$. Permutacija na levi strani enakosti π_{gh} pošlje $x \mapsto (gh) \cdot x$, na desni strani $\pi_g \cdot \pi_h$ pa najprej uporabimo permutacijo π_h, nato pa še permutacijo π_g in tako pošljemo $x \overset{\pi_h}{\longmapsto} h \cdot x \overset{\pi_g}{\longmapsto} g \cdot (h \cdot x)$. Preverjanje, ali je π homomorfizem grup, nas privede do tega, da moramo preveriti, ali v grupi velja zakon asociativnosti: $(gh) \cdot x = g \cdot (h \cdot x)$. Ker je to del definicije grupe, enakost seveda drži.

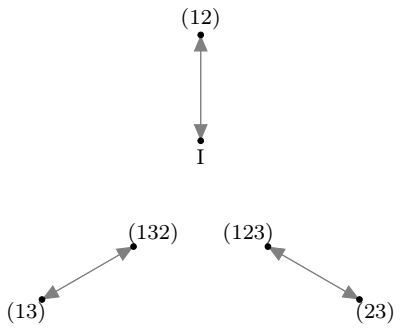
Preveriti moramo še, ali je preslikava zvesta. Za to bo dovolj pokazati, da noben element grupe G, ki ni identiteta, ni preslikan v trivialno permutacijo: če je $g \in G \backslash \{e\}$, potem je $g \cdot e = g$, torej je $\pi_g(e) = g$. Iz tega sledi, da π_g ni identična oziroma trivialna permutacija. ∎

Dokaz Cayleyjevega izreka prikaže konstrukcijo reprezentacije grupe G kot grupe permutacij same sebe. Za lažje razumevanje si oglejmo, kako te permutacije izgledajo v nekaj konkretnih primerih.

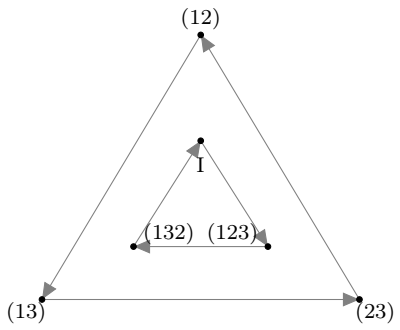
Primer 3.12. Začnimo z grupo permutacij S_3 množice $[3] = \{1, 2, 3\}$. Grupa S_3 ima 6 elementov $\{\mathrm{id}, (12), (13), (23), (123), (132)\}$, ki so na slikah 1a in 1b prikazani kot disjunktna vozlišča. Na sliki 1a je prikazana permutacija grupe S_3, ki jo inducira transpozicija (12), kot je to opisano v dokazu Cayleyjevega osnovnega izreka. Zanimajo nas torej permutacije, asociirane k $(12) \in S_3$:

$$(12) \mapsto \pi_{(12)} \in S_3,$$
$$\pi_{(12)}(h) = (12) \cdot h \text{ za vsak } h \in S_3.$$

Posamezna permutacija je na sliki 1a prikazana s puščico, katere začetek je v elementu $h \in S_3$ in konec v $\pi_{(12)}(h)$.



(a) Permutacija grupe S_3, inducirana s transpozicijo (12).



(b) Permutacija grupe S_3, inducirana s permutacijo (123).

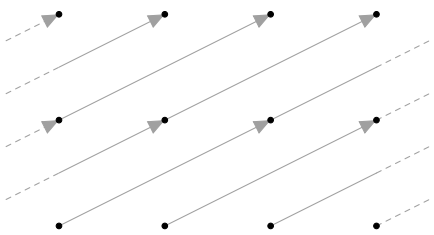
Slika 1: Permutaciji grupe S_3, inducirani z (12) in (123).

Na sliki 1b pa je prikazana permutacija grupe S_3, inducirana z (123), s puščicami pa so prikazane naslednje permutacije:

$$(123) \mapsto \pi_{(123)} \in S_3,$$
$$\pi_{(123)}(h) = (123) \cdot h \text{ za vsak } h \in S_3.$$

Primer 3.13. Dokaz Cayleyjevega osnovnega izreka deluje tako za končne kot tudi za neskončne grupe. Zato si oglejmo še primer, v katerem nastopa neskončna grupa. Obravnavajmo produkt dveh kopij grupe celih števil $G = \mathbb{Z} \times \mathbb{Z}$. Tu so posamezni elementi predstavljeni z urejenimi pari celih števil, binarno operacijo na G pa vpeljemo s seštevanjem po koordinatah: $(a, b) + (c, d) = (a + b, c + d)$.

Na sliki 2 smo po zgledu primera 3.12 za vozlišča postavili elemente G, le-ti tvorijo celoštevilsko mrežo v ravnini. Puščice na sliki pa predstavljajo permutacije elementov množice $\mathbb{Z} \times \mathbb{Z}$, ki so nastale s pomočjo elementa $(2, 1)$. Bolj natančno to pomeni, da če je $h \in G$, kjer je $h = (h_1, h_2)$, potem so s puščico prikazane permutacije grupe G, inducirane z elementom $(2, 1)$, ki imajo začetek v h in konec v $(2, 1) + h$.



Slika 2: Delovanje $(2, 1)$ na $\mathbb{Z} \times \mathbb{Z}$.

3.2 Orbite in stabilizatorji

V tem poglavju bomo predstavili pojme, ki pogosto pridejo zelo prav pri preučevanju delovanja grup. Delovanja grup lahko razstavimo na orbite, kar vodi do prostora orbit delovanja. Večkrat pa lahko postopamo tudi obratno in poskušamo razumeti celoten objekt preko prostora orbit in stabilizatorjev. Ta razdelek je povzet po knjigah [9] in [10].

Definicija 3.14. Naj bo X nek matematični objekt, kot na primer množica, graf, pravilni mnogokotnik. Naj G deluje na objekt X. Če je $x \in X$, potem je

$$\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$$

stabilizator elementa x.

Lema 3.15. *Za vsako delovanje G na matematični objekt X in za vsak $x \in X$ je* $\mathrm{Stab}(x)$ *podgrupa grupe G.*

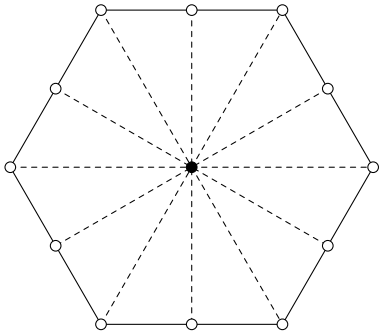
Dokaz: Da bi pokazali, da je množica $\mathrm{Stab}(x)$ podgrupa grupe G je dovolj pokazati, da je množica $\mathrm{Stab}(x)$ zaprta za produkte in inverze. S kompozitumom dveh simetrij, ki fiksirata x, tvorimo simetrijo, ki še vedno fiksira x. Torej je množica $\mathrm{Stab}(x)$ zaprta za produkte. Inverz simetrije, ki fiksira x, prav tako fiksira x. Posledično je množica $\mathrm{Stab}(x)$ zaprta tudi za inverze. Iz tega sledi, da je $\mathrm{Stab}(x)$ res podgrupa grupe G. ∎

Zgled 3.16. Diedrska grupa D_n deluje na pravilni n-kotnik. Če je x oglišče tega večkotnika ali pa razpolovišče katerekoli stranice v tem večkotniku, je $\mathrm{Stab}(x) \cong \mathbb{Z}_2$, saj množica $\mathrm{Stab}(x)$ vsebuje le identiteto in zrcaljenje skozi premico, ki poteka skozi x. Opazimo še:

- Če sta x in x' oglišči, ki si nista nasproti v večkotniku, potem velja, da $\mathrm{Stab}(x) \neq \mathrm{Stab}(x')$.
- Če je x središče pravilnega n-kotnika, potem je $\mathrm{Stab}(x) = D_n$, saj vsebuje točno vse simetrije, ki se nahajajo v diedrski grupi D_n.
- Če je x točka, ki ni oglišče ali ni razpolovišče stranice večkotnika ali ni na premici, ki povezuje središče n-kotnika z ogliščem ali razpoloviščem stranice, potem vsebuje stabilizator takšnega oglišča x le identiteto.

Oglejmo si pravkar ugotovljeno na pravilnem šestkotniku na sliki 3. Nanj deluje diedrska grupa D_6. Stabilizator belih točk šestkotnika na sliki 3 je izomorfen $\mathbb{Z}_2$. Stabilizator središča šestkotnika je kar celotna grupa D_6. Vsaka točka, ki ni posebej označena na sliki in ki ne leži na eni od črtkanih daljic našega šestkotnika, ima trivialen stabilizator.

Zgled 3.17. Naj grupa S_n deluje na množico $[n] = \{1, 2, ..., n\}$. Potem je $\mathrm{Stab}(i) \cong S_{n-1}$ za vsak $i \in [n]$.



Slika 3: Delovanje diedrske grupe D_6 na pravilni šestkotnik in iskanje stabilizatorjev posameznih točk.

Definicija 3.18. Naj grupa G deluje na matematični objekt X. Če ima nek $x \in X$ trivialen stabilizator, $\mathrm{Stab}(x) = \{e\}$, potem rečemo, da je x *premaknjen prosto* z delovanjem grupe G.

Definicija 3.19. Naj grupa G deluje na objekt X. *Množica negibnih točk* glede na element grupe $g \in G$ je dana z

$$X^g := \{x \in X \mid g \cdot x = x\}.$$

Zgled 3.20. Naj bo R podgrupa v diedrski grupi D_n, ki vsebuje vse rotacije te grupe. S $\mathcal{P}$ označimo pravilni n-kotnik in s $\partial\mathcal{P}$ rob tega n-kotnika, ki je sestavljen iz n oglišč in n stranic. Delovanje R na $\partial\mathcal{P}$ je prosto, medtem ko delovanje R na $\mathcal{P}$ ni prosto. V zadnjem primeru je problematično središče c danega n-kotnika, saj ga vsaka rotacija fiksira in velja, da je $\mathrm{Stab}(c) = R$.

Definicija 3.21. Naj grupa G deluje na objekt X in naj bo $x \in X$. Potem je

$$\mathrm{Orb}(x) = \{g \cdot x \mid g \in G\}$$

orbita elementa x.

Zgled 3.22. Naj bo $Q = [0,1]^2$ poln kvadrat v $\mathbb{R}^2$ in G grupa izometrij kvadrata Q glede na evklidsko metriko v $\mathbb{R}^2$. Potem G naravno deluje na Q preko izometrij in vemo, da je grupa $G \cong D_4$.

- Naj bo $t \in G$ zrcaljenje preko diagonale skozi oglišči kvadrata $(0,0)$ in $(1,1)$. Potem je množica negibnih točk $Q^t = \{(x,x) \mid x \in [0,1]\}$.
- Naj bo $s \in G$ rotacija za $\frac{\pi}{2}$. Potem je množica negibnih točk $Q^s = \{(\frac{1}{2}, \frac{1}{2})\}$.
- Orbita elementa $(0,0)$ so vsa štiri oglišča kvadrata Q in stabilizator elementa $(0,0)$ je enak množici $\{\mathrm{id}_Q, t\}$.

- Stabilizator elementa $(\frac{1}{3}, 0)$ je trivialna množica.
- Stabilizator elementa $(\frac{1}{2}, \frac{1}{2})$ je enak množici vseh elementov v grupi G.

Zgled 3.23. Orbita vsakega oglišča na pravilnem n-kotniku pod delovanjem grupe D_n je množica vseh oglišč. Če je x razpolovišče stranice v pravilnem n-kotniku, potem je njegova orbita množica vseh razpolovišč stranic v pravilnem n-kotniku.

Izrek 3.24. *Naj bo dano delovanje grupe G na objekt X in naj bo dan nek $x \in X$. Potem obstaja bijekcija med množico* $\mathrm{Orb}(x)$ *in levim odsekom* $\mathrm{Stab}(x)$*, dana z*

$$g \cdot x \longleftrightarrow g \cdot \mathrm{Stab}(x).$$

Opomba 3.25. Spomnimo se, da je levi odsek podgrupe H grupe G glede na element $g \in G$ enak množici $gH = \{g \cdot h \mid h \in H\}$.

Dokaz: Dano je delovanje grupe G na X in nek $x \in X$. Potem velja enakost $g \cdot x = h \cdot x$, če in samo če je $g^{-1}h \cdot x = x$, to pa velja natanko tedaj, ko je $g^{-1}h \in \mathrm{Stab}(x)$. Iz tega sledi, da velja $g \cdot x = h \cdot x$, če in samo če sta leva odseka $g \cdot \mathrm{Stab}(x)$ in $h \cdot \mathrm{Stab}(x)$ enaka. ∎

Iz izreka 3.24 dobimo naslednjo posledico, ki se izkaže za uporabno pri izračunu moči končnih grup.

Posledica 3.26 (Izrek orbita-stabilizator)**.** *Naj bo G končna grupa, ki deluje na X. Potem za vsak $x \in X$ velja naslednja enakost:*

$$|G| = |\,\mathrm{Stab}(x)| \cdot |\,\mathrm{Orb}(x)|.$$

Dokaz: Moč grupe G je enaka produktu moči $\mathrm{Stab}(x)$ in indeksa podgrupe $\mathrm{Stab}(x)$ v grupi G. Ampak indeks podgrupe $\mathrm{Stab}(x)$ je ravno število vseh levih odsekov $\mathrm{Stab}(x)$, le-to pa je po izreku 3.24 ravno moč množice $\mathrm{Orb}(x)$.

∎

S pomočjo izreka 3.24 dobimo zanimivo metodo za identificiranje elementov v grupi z elementi v orbiti elementa $x \in X$, ko je njegov stabilizator trivialen.

Posledica 3.27. *Naj grupa G deluje na matematični objekt X. Za vsak $x \in X$, ki ima trivialen stabilizator,* $\mathrm{Stab}(x) = \{e\}$*, obstaja bijektivna preslikava med elementi grupe G in elementi* $\mathrm{Orb}(x)$.

3.3 Osnovno o grafih

Eden ključnih vpogledov v teorijo grup je ta, da lahko grupe preučujemo preko grup simetrij grafov. To nam omogoči, da lahko grupe obravnavamo kot neke geometrijske objekte. Kako nekatere grupe delujejo na grafe, si bomo bolj podrobno ogledali v nadaljevanju magistrskega dela, v tem poglavju pa vpeljimo še nekaj terminologije in značilnosti, s katerimi se srečujemo v teoriji grafov. Ta razdelek je povzet po knjigah [7], [10] in [11].

Definicija 3.28. *Graf* Γ je sestavljen iz *množice vozlišč* $V(\Gamma)$ in *množice povezav* $E(\Gamma)$, kjer je vsaka povezava predstavljena kot neurejen par vozlišč s pomočjo funkcije k, ki poda krajišči dane povezave: $k(e) = \{u, v\}$, kjer so $u, v \in V(\Gamma)$ in $e \in E(\Gamma)$. V tem primeru rečemo, da sta u in v *sosednji* vozlišči. Večkrat označimo povezavo e kar z uv in s tem takoj nakažemo, da ima povezava e krajišči u in v.

Grafe najpogosteje predstavimo tako, da vozlišča označimo s točkami, povezave pa z loki ali daljicami med posameznimi točkami.

Lahko se zgodi, da imata dve povezavi enaki krajišči. To pomeni, da dovolimo večkratne povezave med istim parom sosednjih vozlišč, takim povezavam pa pravimo *vzporedne povezave*. Dovolimo lahko tudi *zanke*, to so povezave, ki imajo obe krajišči enaki. Grafom, v katerih lahko pride do vzporednih povezav in zank, bomo rekli *multigrafi*. Grafi brez zank in večkratnih povezav pa se imenujejo *enostavni grafi*. Če ne bo posebej poudarjeno, bomo z besedo graf imeli v mislih enostaven graf.

Definicija 3.29. *Stopnja vozlišča* u v grafu Γ je enaka številu povezav grafa Γ, ki imajo točko u za svoje krajišče. Označimo jo z $\deg_\Gamma(u)$. V enostavnih grafih vozliščem stopnje 0 pravimo *izolirana vozlišča*, vozliščem stopnje 1 pa *listi*.

Najmanjšo stopnjo vozlišča grafa Γ označimo z $\delta(\Gamma)$, največjo stopnjo pa z $\Delta(\Gamma)$. Graf Γ je *regularen*, če velja $\delta(\Gamma) = \Delta(\Gamma)$, torej ima vsako vozlišče v tem grafu enako stopnjo. Graf je *d-regularen*, če velja $d = \delta(\Gamma) = \Delta(\Gamma)$.

Stopnje vozlišč in število povezav v enostavnem grafu veže naslednja enakost:

Lema 3.30 (Lema o rokovanju)**.** *Za vsak enostaven graf* Γ *velja*

$$\sum_{v \in V(\Gamma)} \deg_\Gamma(v) = 2 \cdot |E(\Gamma)|.$$

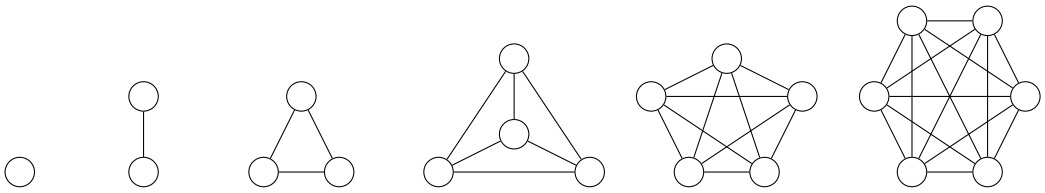
Lema velja, ker ima vsaka povezava dve krajišči, zato k vsoti vseh prispeva natanko 2. Od kod ime leme o rokovanju? Zamislimo si graf, katerega vozlišča predstavljajo osebe na zabavi, povezava med vozliščema pa simbolizira rokovanje med dvema osebama. Vsota stopenj točk je število vseh rok, ki so bile udeležene v rokovanjih, medtem, ko je število rokovanj enako številu povezav v grafu. V vsakem rokovanju sta bili udeleženi dve roki, zato je število rok dvakrat večje, kot je število rokovanj.

Iz leme o rokovanju sledi, da ima vsak enostaven graf sodo mnogo točk lihe stopnje.

Definicija 3.31. Graf Γ je *dvodelni*, če lahko množico točk $V(\Gamma)$ zapišemo kot disjunktno unijo dveh podmnožic $A, B \subseteq V(\Gamma)$ tako, da je za vsako povezavo $uv \in E(\Gamma)$ ena od točk u, v vsebovana v množici A, druga pa v množici B. Množici A in B imenujemo *množici dvodelnega razbitja* grafa Γ.

V teoriji grafov poznamo veliko družin enostavnih grafov. Oglejmo si nekatere od njih:

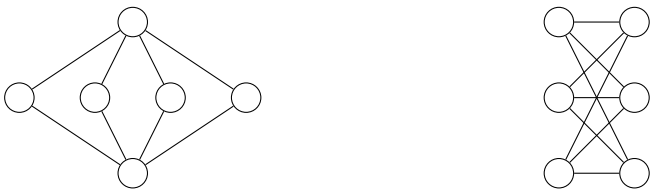
- *Ničelni graf* je graf brez povezav.
- *Polni graf* K_n na n vozliščih ima natanko eno povezavo, ki povezuje vsak par različnih si vozlišč, torej ima $\binom{n}{2} = \frac{n(n-1)}{2}$ povezav. Polni grafi K_n so $(n-1)$-regularni za vsak $n \in \mathbb{N}$.



(a) K_1 (b) K_2 (c) K_3 (d) K_4 (e) K_5 (f) K_6

Slika 4: Polni grafi za $n \in \{1, 2, 3, 4, 5, 6\}$.

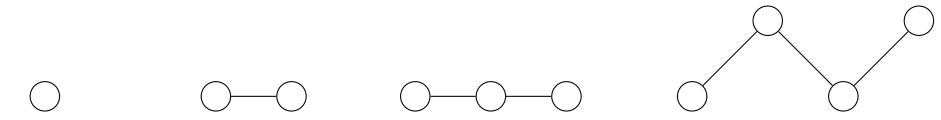
- *Polni dvodelni graf* $K_{m,n}$ je enostaven graf, katerega vozlišča so razdeljena v dve disjunktni množici A in B. V prvi množici je m vozlišč, v drugi pa n vozlišč. Vsako vozlišče v množici A je povezano z vsakim vozliščem v množici B. Torej je množica povezav $E(K_{m,n}) = \{uv \mid u \in A, v \in B\}$. Polni dvodelni graf $K_{m,n}$ ima $m + n$ vozlišč in mn povezav. Zanj velja, da sta $\delta(K_{m,n}) = \min\{m, n\}$ in $\Delta(K_{m,n}) = \max\{m, n\}$. Graf $K_{m,n}$ je regularen natanko tedaj, ko je $m = n$.



(a) $K_{2,4}$ (b) $K_{3,3}$

Slika 5: Polna dvodelna grafa $K_{2,4}$ in $K_{3,3}$.

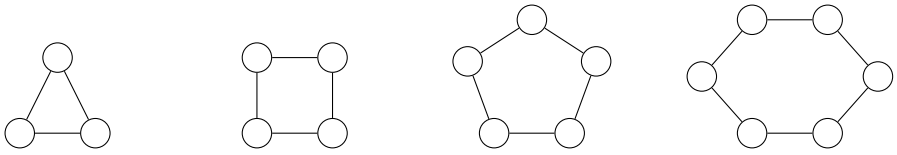
- *Pot* P_n dolžine $n-1$ ima n različnih vozlišč $v_1, ..., v_n$, množica povezav $E(P_n)$ sestoji iz povezav oblike $\{v_j, v_{j+1}\}$ za vsak $j \in \{1, ..., n-1\}$. Pot P_n ima torej n vozlišč in $n-1$ povezav. Če je $n < \infty$, potem rečemo, da ta pot povezuje vozlišči v_1 in v_n. Za $n \geq 3$ velja, da sta $\delta(P_n) = 1$ in $\Delta(P_n) = 2$.



(a) P_1 (b) P_2 (c) P_3 (d) P_4

Slika 6: Poti P_1, P_2, P_3, P_4.

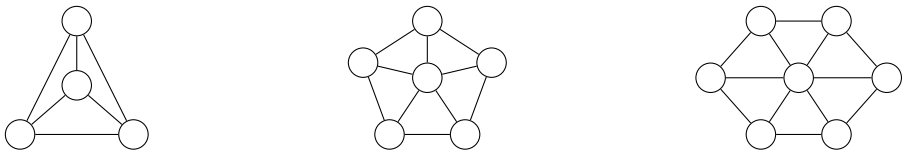
- *Cikel* C_n dolžine n, kjer je $n \geq 3$, ima množico n različnih si vozlišč $v_1, ..., v_n$, množica povezav cikla C_n sestoji iz povezav $\{v_j, v_{j+1}\}$ za $j \in \{1, ..., n-1\}$ in povezave $\{v_1, v_n\}$. Cikel C_n ima n vozlišč in n povezav. Je 2-regularen in je dvodelni natanko tedaj, ko je n sodo število. Kadar dopuščamo tudi multigrafe, sta definirana še cikla C_1, ki je *zanka* in C_2, ki predstavlja *par vzporednih povezav*.



(a) C_3 (b) C_4 (c) C_5 (d) C_6

Slika 7: Cikli C_3, C_4, C_5, C_6.

- *Kolo* W_n, kjer je $n \geq 3$, je graf z množico vozlišč $V(W_n) = \{v_1, ..., v_n, v_\infty\}$ ter množico povezav $E(W_n) = \{\{v_i, v_{i+1}\}, \{v_i, v_\infty\} \mid i \in \{1, ..., n\}\}$. Graf W_n ima $n+1$ točk in $2n$ povezav.



(a) W_3 (b) W_5 (c) W_6

Slika 8: Kolesa W_3, W_5, W_6.

Definicija 3.32. Graf je *povezan*, če je mogoče priti iz vsakega vozlišča v vsako drugo vozlišče po kakšni poti v grafu.

V nadaljevanju magistrskega dela se bomo veliko ukvarjali z grupami, ki so povezane z *drevesi*. Zato si poglejmo definicijo tega enostavnega grafa in preko trditve 3.34 še karakterizacijo dreves.

Definicija 3.33. *Drevo* je povezan graf, ki ne vsebuje ciklov.

Trditev 3.34. *Graf* Γ *je drevo natanko tedaj, ko za vsak par vozlišč v grafu* Γ *obstaja natanko ena pot, ki ti dve vozlišči povezuje.*

Dokaz: Recimo, da je Γ drevo. Torej je Γ povezan in vsaki dve vozlišči lahko povežemo s potjo v Γ. Recimo, da obstajata vozlišči u in v, ki ju lahko povežemo z dvema različnima potema p_1 in p_2. Iz teh dveh poti lahko konstruiramo cikel v grafu Γ tako, da poiščemo prvo vozlišče, kjer se poti ločita in nato prvo vozlišče, kjer se ti dve poti spet srečata. Obe poti med tema dvema vozliščema tvorita cikel. To pa je v protislovju z dejstvom, da je Γ drevo, torej povezan graf brez ciklov. Iz tega sledi, da lahko poljubni dve vozlišči v drevesu Γ povežemo z natanko eno potjo.

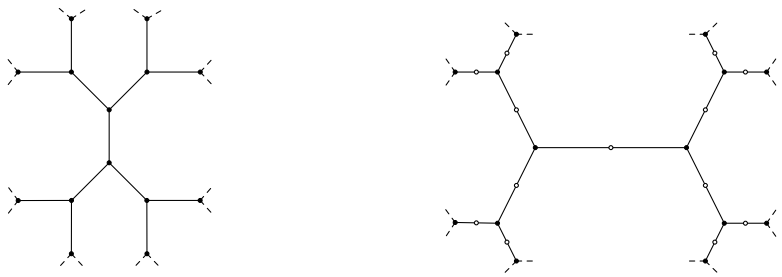
Sedaj pa naj bo Γ tak graf, za katerega velja, da lahko vsak par vozlišč povežemo z natanko eno potjo v Γ. Iz tega takoj sledi, da je Γ povezan graf. Recimo, da graf Γ vsebuje cikel $v_1, ..., v_n$. Ker je $n \geq 3$, sta poti v_1, v_n in $v_1, v_2, ..., v_n$ različni in obe povezujeta v_1 z v_n. To pa je v protislovju z zgornjim dejstvom, da lahko vsak par vozlišč povežemo z natanko eno potjo v grafu. Iz tega sledi, da je Γ povezan graf, ki ne vsebuje ciklov, torej je Γ drevo. ∎

V teoriji grafov obstaja vrsta zanimivih rezultatov o končnih drevesih, nas pa bodo predvsem zanimala neskončna drevesa, saj bomo kasneje raziskali grupe, ki delujejo na določena neskončna drevesa.

Definicija 3.35. *Regularno m-drevo* je drevo s fiksno stopnjo vozlišč m. Za dano vrednost m obstaja le eno regularno m-drevo, ki ga označimo s τ_m. Če je $m = 1$, bo 1-drevo sestavljeno iz dveh vozlišč in povezave med njima, torej bo to drevo izgledalo kot pot P_2. Če pa je $m = 0$, dobimo množico izoliranih vozlišč. Opazimo lahko, da je drevo τ_m neskončno, ko je $m \geq 2$.

Drevo je *biregularno*, če je dvodelno in če imajo vsa vozlišča v posameznem delu dvodelnega drevesa fiksno stopnjo vozlišč - v enem delu m, v drugem delu grafa pa n. Če imamo dani stopnji vozlišč m in n, potem obstaja le eno biregularno drevo, ki ga označimo s $\tau_{m,n}$.

Na sliki 9 sta prikazana primera regularnega in biregularnega drevesa.



(a) Regularno 3-drevo τ_3. (b) Biregularno drevo $\tau_{2,3}$.

Slika 9: Primer regularnega in biregularnega drevesa.

Definicija 3.36. *Usmerjen graf* je sestavljen iz množice vozlišč V in množice povezav E, ki vsebuje urejene pare vozlišč. Vsaka povezava v usmerjenem grafu ima

začetno in *končno* vozlišče. Smer povezave je grafično prikazana s puščico na povezavi, ki kaže proti končnemu vozlišču. Usmerjen graf je povezan, če je pripadajoč neusmerjen graf povezan.

3.4 Grupe simetrij grafov

Mnoge pomembne končne grupe se pojavijo kot grupe simetrij geometrijskih objektov. Najbolj značilen zgled so diedrske grupe, saj so to grupe simetrij pravilnih n-kotnikov. Cilj tega razdelka je raziskati grupe simetrij grafov malce bolj podrobno. Razdelek je povzet po osnovnem gradivu magistrske naloge [10] in zapiskov s predavanj [6].

Definicija 3.37. *Simetrija* grafa Γ je bijekcija α, ki slika vozlišča v vozlišča in povezave v povezave tako, da velja: če sta krajišči povezave $e \in E(\Gamma)$ vozlišči $\{u, v\}$, potem sta krajišči povezave $\alpha(e)$ vozlišči $\{\alpha(u), \alpha(v)\}$. *Grupa simetrij grafa* Γ je zbirka vseh njegovih simetrij. Označimo jo s $\mathrm{Sym}(\Gamma)$.

Opomba 3.38. V teoriji grafov ponavadi takšni simetriji pravijo avtomorfizem grafa in zbirki vseh avtomorfizmov danega grafa grupa avtomorfizmov grafa.

Naj bo Γ enostaven, končen, neusmerjen graf z množico vozlišč $V(\Gamma)$ in množico povezav $E(\Gamma)$. Na avtomorfizem grafa lahko gledamo tudi kot na permutacijo množice vozlišč, ki ohranja sosednost vozlišč. Torej je grupa avtomorfizmov grafa Γ množica vseh permutacij množice vozlišč $V(\Gamma)$, ki ohranjajo sosednost vozlišč:

$$\mathrm{Aut}(\Gamma) = \{\pi \in \mathrm{Sym}(V(\Gamma)) \mid \{u, v\} \in E(\Gamma) \Leftrightarrow \{\pi(u), \pi(v)\} \in E(\Gamma)\}.$$

Če je π bijekcija, ki preslika množico $V(\Gamma)$ samo vase, potem π inducira bijekcijo na podmnožicah moči 2 množice $V(\Gamma)$, zatorej imata $\pi(E(\Gamma))$ in $E(\Gamma)$ enako moč. Če je π avtomorfizem, potem mora π nujno ohraniti tudi nesosednost vozlišč. Zato je naša prvotna definicija 3.37 ekvivalentna zgornji, ki na avtomorfizem grafa gleda kot na permutacijo množice vozlišč, ki ohranja sosednost in nesosednost vozlišč. Če je $\pi \in \mathrm{Aut}(\Gamma)$, potem π ohranja sosednost in sosede vozlišča u pošlje v sosede vozlišča $\pi(u)$. Iz tega sledi, da imata u in $\pi(u)$ enako stopnjo vozlišča. Ker je kompozitum dveh avtomorfizmov spet avtomorfizem, je množica vseh avtomorfizmov grafa grupa simetrij grafa.

Definicija 3.39. Naj bo $A \leq \mathrm{Sym}(X), B \leq \mathrm{Sym}(Y)$, kjer sta množici X, Y disjunktni. Njuna *vsota* oziroma *direktni produkt* $A + B$ je grupa permutacij

$$A + B = \{(\alpha, \beta) \mid \alpha \in A,\, \beta \in B\},$$

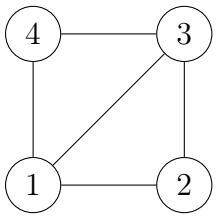
ki deluje na disjunktno unijo $X \cup Y$ po pravilu:

$$(\alpha, \beta)(z) = \begin{cases} \alpha(z), & z \in X, \\ \beta(z), & z \in Y. \end{cases}$$

Velja, da je $A + B \leq \mathrm{Sym}(X \cup Y)$ in $A + B$ ima $|A| \cdot |B|$ elementov.

Primer 3.40. Hitro je razvidno, da je simetrijska grupa polnega grafa K_n izomorfna simetrični grupi S_n, saj je vsaka permutacija vozlišč grafa K_n avtomorfizem grafa.

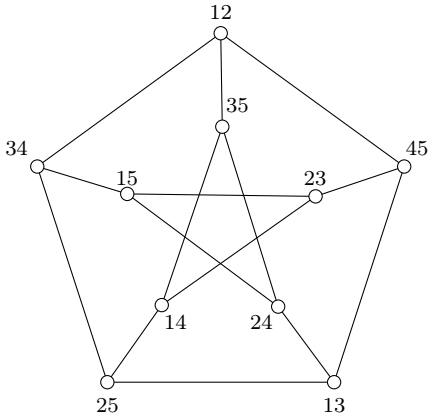
Zamislimo si sedaj še graf K_4 brez ene povezave, kjer je njegova množica vozlišč $V = \{1, 2, 3, 4\}$ in kjer je odstranjena povezava $\{2, 4\}$. Zamišljeni graf je prikazan na sliki 10. Potem je grupa avtomorfizmov danega grafa enaka $A = \{\mathrm{id}, (13), (24), (13)(24)\}$ in zato je $A = S_2 + S_2$.



Slika 10: K_4 brez povezave $\{2, 4\}$.

Primer 3.41. Dokažimo, da je celotna grupa avtomorfizmov Petersenovega grafa izomorfna simetrični grupi S_5.

Naj bo Γ Petersenov graf. Zanj velja, da so njegova vozlišča podmnožice moči 2 množice $\{1, 2, 3, 4, 5\}$, kjer sta vozlišči u in v sosednji, če in samo če sta si disjunktni. Z ij označimo vozlišče $\{i, j\}$. Na sliki 11 je opisani graf tudi prikazan.



Slika 11: Petersenov graf.

Vsak element $\pi \in S_5$ inducira permutacijo množice dvoelementnih podmnožic množice $\{1, 2, 3, 4, 5\}$. To pomeni, da inducira permutacijo $\overline{\pi}$ grafa Γ. Na primer, če je $\pi = (134)(25) \in S_5$, potem $\overline{\pi}$ pošlje vozlišče $\{1, 2\}$ v vozlišče $\{3, 5\}$. V tem primeru je $\overline{\pi} = (12, 35, 42, 15, 32, 45)(13, 34, 41)(25) \in \mathrm{Sym}(V)$, kjer je V množica vozlišč Petersenovega grafa Γ. Še več, vidimo lahko, da različni elementi S_5 inducirajo različne permutacije množice V. Vsaka od teh induciranih permutacij je avtomorfizem grafa Γ, ker za vsa $\pi \in S_5$ velja, da sta $u, v \in V$ disjunktni, če in samo

če sta $\pi(u)$ in $\pi(v)$ disjunktni vozlišči. Zato je preslikava

$$\begin{aligned}\phi\colon S_5 &\to V,\\ \pi &\mapsto \overline{\pi},\end{aligned}$$

injektivni homomorfizem grup v $\mathrm{Aut}(\Gamma)$. Zato tudi velja naslednje: $S_5 \cong \phi(S_5) \leq \mathrm{Aut}(\Gamma)$.

Pokažimo sedaj, da $\phi(S_5)$ ni le podgrupa grupe $\mathrm{Aut}(\Gamma)$, ampak kar celotna grupa avtomorfizmov Petersenovega grafa Γ. Za slednje zadošča pokazati, da je $\mathrm{Aut}(\Gamma)$ podgrupa grupe $\phi(S_5)$. Naj bo $\pi \in \mathrm{Aut}(\Gamma)$ poljuben avtomorfizem Petersenovega grafa Γ. Pokažimo, da obstaja tak $\overline{g} \in \phi(S_5)$, da velja $\pi\overline{g} = \mathrm{id}$. To bi impliciralo, da je $\pi = \overline{g}^{-1} \in \phi(S_5)$.

Naj bo $\pi\colon \{1,2\} \mapsto \{a,b\}$. Naj $g_1 \in S_5$ preslika a v 1 in b v 2. Potem $\pi\overline{g_1}$ fiksira vozlišče 12 in zatorej permutira svoje sosede $34, 35, 45$. Ločimo primere:

1. Recimo, da $\pi\overline{g_1}$ fiksira vse tri sosede $34, 35, 45$. Torej $\pi\overline{g_1}$ permutira sosede vozlišča 35, kar pomeni, da bodisi vozlišči 14 in 24 fiksira bodisi ju zamenja:

   1.1 Če $\pi\overline{g_1}\colon 14 \mapsto 14$, potem je vozlišče 15 poslano v vozlišče, ki je sosednje 34 in ki ni sosednje 14, torej je 15 fiksirano vozlišče. Podobno lahko vidimo, da so tudi ostala vozlišča fiksirana in zato velja $\pi\overline{g_1} = \mathrm{id}$. Posledično je $\pi \in \phi(S_5)$.

   1.2 Če $\pi\overline{g_1}\colon 14 \mapsto 24$, s tem zamenjamo vozlišči 14 in 24. Vozlišče 15 je poslano v soseda vozlišča $\pi\overline{g_1}(24)$. To pomeni, da je 15 poslano v 25. Vidimo, da $\pi\overline{g_1}$ zamenja 14 in 24, 15 in 25 in pa tudi 13 in 23, preostala vozlišča pa fiksira. Tako je $\pi\overline{g_1} = \overline{g_2}$, kjer je $g_2 = (12)$. Posledično je $\pi \in \phi(S_5)$.

2. Recimo sedaj, da $\pi\overline{g_1}$ fiksira natanko dve vozlišči od vozlišč $34, 35, 45$. Ampak ta primer ni mogoč, saj če fiksira dva od treh vozlišč, mora tudi tretjega, drugače ne ohrani (ne)sosednosti.

3. Recimo, da $\pi\overline{g_1}$ fiksira eno od vozlišč $34, 35, 45$. Naj bo fiksirano vozlišče 34. To pomeni, da $\pi\overline{g_1}$ zamenja vozlišči 45 in 35. Naj bo $g_2 = (34) \in S_5$. Potem $\pi\overline{g_1 g_2}$ ustreza pogojem v prvem primeru zgoraj.

4. Recimo, da $\pi\overline{g_1}$ ne fiksira nobenega od vozlišč $34, 35, 45$. Torej je $(34, 35, 45)$ 3-cikel. Naj bo $g_2 = (34)$. Potem je $\pi\overline{g_1 g_2} = (34, 35)(45)$ in naš problem smo prevedli na tretji primeru zgoraj.

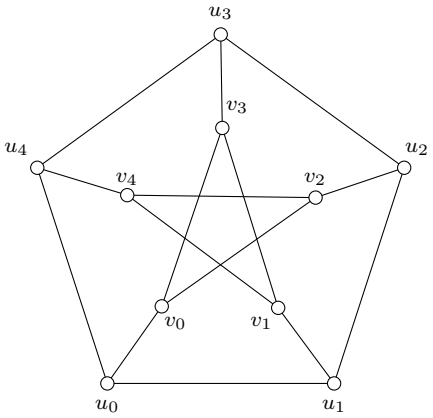
Zgornji primeri nakažejo, da če je $\pi \in \mathrm{Aut}(\Gamma)$, potem obstajajo takšni $g_1, ..., g_r \in S_5$ za neko nenegativno celo število r, da velja: $\pi\overline{g_1}...\overline{g_r} = \mathrm{id}$. Iz tega sledi, da je $\pi \in \phi(S_5)$. Torej je res $\mathrm{Aut}(\Gamma) \cong \phi(S_5) \cong S_5$.

Definicija 3.42. Naj bo G podgrupa simetrijske grupe grafa Γ.

Potem je G *tranzitivna po vozliščih* ali *vozliščno tranzitivna*, če za vsaki dve vozlišči v, v' grafa Γ obstaja taka simetrija $\alpha \in G$, da je $\alpha(v) = v'$.

Grupa G je *tranzitivna po povezavah* ali *povezavno tranzitivna*, če za vsaki dve povezavi e, e' grafa Γ obstaja simetrija $\alpha \in G$ tako, da velja $\alpha(e) = e'$.

Primer 3.43. Vrnimo se k Petersenovem grafu. Označimo ga z Γ. Če raziščemo simetrije grafa Γ na sliki 12, vidimo, da je diedrska grupa D_5 prava podgrupa simetrijske grupe $\mathrm{Sym}(\Gamma)$. Pokažimo, da je simetrijska grupa Γ tranzitivna na vozliščih in sicer tako, da poiščemo še simetrijo, ki zamenja množico 'notranjih' z množico 'zunanjih' vozlišč.



Slika 12: Petersenov graf drugič.

Zunanja vozlišča na Petersenovem grafu Γ smo označili z u_i in notranja vozlišča z v_i, kjer je $i \in \{0, 1, 2, 3, 4\}$. Poiščimo sedaj avtomorfizem, ki zamenja zunanja in notranja vozlišča. Ta avtomorfizem mora preslikati u_0 v v_0, u_1 v v_2 in u_2, ki je sosed u_1, v v_4. Če nadaljujemo ta način zamenjave vozlišč, ugotovimo, da se u_2 preslika v v_4, u_3 v v_1 ter u_4 v v_3. Podobno se v_0 preslika v u_0, v_1 v u_2, v_2 v u_4, v_3 v u_1 in v_4 v u_3. To lahko zapišemo tudi kot

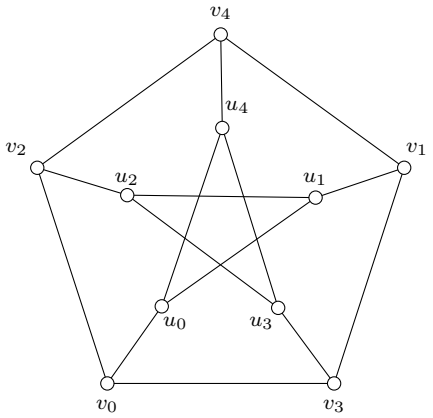
$$u_i \mapsto v_{2i \pmod 5},$$
$$v_i \mapsto u_{2i \pmod 5}.$$

Zapišimo še iskani avtomorfizem

$$\sigma(\Gamma) = (u_0v_0)(u_1v_2u_4v_3)(u_2v_4u_3v_1).$$

Oglejmo si to zamenjavo vozlišč še na spodnji sliki 13.

Dokažimo, da je preslikava σ res avtomorfizem grafa Γ. Le-ta mora ohranjati sosednost vozlišč. Sosedi vozlišča u_i so $u_{i\pm1 \pmod 5}$ in v_i, kjer je $i \in \{0, 1, 2, 3, 4\}$. S preslikavo dobimo $\sigma(u_i) = v_{2i \pmod 5}$, $\sigma(u_{i\pm1 \pmod 5}) = v_{2i\pm2 \pmod 5}$, $\sigma(v_i) = u_{2i \pmod 5}$.



Slika 13: Petersenov graf po zamenjavi notranjih in zunanjih vozlišč.

Vidimo lahko, da se sosedi u_i preslikajo v sosede $\sigma(u_i)$. Sosedi vozlišča v_i so u_i, $v_{i\pm 2 \pmod 5}$. Če na njih uporabimo preslikavo σ, dobimo $\sigma(v_i) = u_{2i}$, $\sigma(v_{i\pm 2 \pmod 5}) = u_{2i\pm 4 \pmod 5}$ in $\sigma(u_i) = v_{2i \pmod 5}$. Tudi tu se izkaže, da se sosedi vozlišča v_i preslikajo v sosede vozlišča $\sigma(v_i)$.

Označimo množico zbranih simetrij iz diedrske grupe D_5 in simetrije σ, ki zamenja zunanja in notranja vozlišča Petersenovega grafa Γ, z G. Pokažimo, da je G tranzitivna na vozliščih. Veljati mora torej, da za vsaki dve vozlišči v, v' grafa Γ obstaja simetrija α grafa Γ v grupi G, da velja $\alpha(v) = v'$. Vidimo, da lahko vsaki dve vozlišči u_i, u_j, kjer sta $i, j \in \{0, 1, 2, 3, 4\}$, preslikamo drugo v drugo z rotacijami ali zrcaljenji iz diedrske grupe D_5. Analogno velja tudi za vsak par vozlišč v_i, v_j. Vozlišča u_i, v_j pa lahko preslikamo drug v drugega s kompozitumom katere od simetrij v diedrski grupi in simetrije σ. Ko to preverimo, vidimo, da je grupa $\mathrm{Sym}(\Gamma)$ res tranzitivna na vozliščih.

Oglejmo si še nekaj zanimivih podgrup grupe simetrij grafov:

Lema 3.44. *Če je Γ usmerjen graf, potem zbirka vseh simetrij grafa Γ, ki ohranjajo usmerjenost vsake povezave v grafu, tvori podgrupo grupe simetrij grafa Γ.*

Dokaz: Da bi pokazali, da je podmnožica grupe podgrupa, je dovolj dokazati, da je podmnožica zaprta za produkte in inverze. Če sta torej g in h simetriji grafa Γ, ki ohranjata usmerjenost povezav, potem to pomeni, da usmerjenost povezav ohranja tudi njun produkt ter njuni inverzi. ∎

Lema 3.45. *Če ima graf Γ oznake na povezavah in/ali vozliščih, potem je zbirka simetrij, ki te oznake ohrani, podgrupa grupe* $\mathrm{Sym}(\Gamma)$.

Dokaz: Dokaz je povsem analogen zgornjemu. ∎

Definicija 3.46. Če ima graf Γ določeno okrasitev, na primer usmerjenost povezave, vozlišča in/ali povezave z oznakami ali določene barve, potem naj $\mathrm{Sym}^+(\Gamma)$ označuje podgrupo $\mathrm{Sym}(\Gamma)$, ki ohrani to okrasitev grafa.

3.5 Množice generatorjev

En način, kako lahko opredelimo grupo, je preko konstrukcije grupe kot grupe avtomorfizmov nekega matematičnega objekta. Vendar je v praksi težko najti ustrezen geometrijski objekt, iz katerega bi nastala grupa s točno določenimi algebraičnimi lastnostmi, ki si jih v iskani grupi želimo. Spoznali bomo, da obstaja še en način za konstrukcijo grup, ki je sicer bolj abstrakten. Pri tem si pomagamo z generatorji grupe. Ta razdelek je povzet po knjigi [10].

Definicija 3.47. Naj bo G grupa in S podmnožica elementov v grupi G. Množica S *generira* G, če lahko vsak element v grupi G predstavimo kot produkt elementov iz množice S in inverzov elementov iz množice S. Potem množici S rečemo *množica generatorjev grupe* G. Zgornje večkrat označimo z $\langle S \rangle = G$. Grupa G je *končno generirana*, če ima končno množico generatorjev.

Poglejmo si nekaj zgledov:

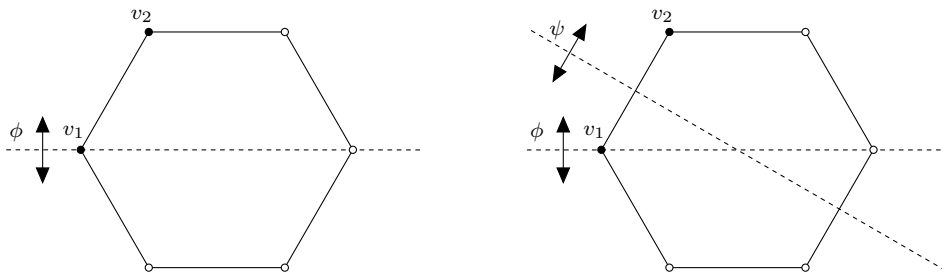
Zgled 3.48. Vsaka končna grupa je končno generirana, saj lahko za množico generatorjev vzamemo kar grupo samo. Vendar pa bo nas zanimalo predvsem, če obstaja kakšna prava podmnožica, ki generira dano grupo. Recimo, da imamo dano simetrično grupo S_n. Množica generatorjev, ki generira to grupo, je množica sosednjih transpozicij, $S = \{(12), (23), ..., (n(n-1))\}$. Dobro znana množica generatorjev grupe S_n je tudi $S = \{(12), (12...n)\}$, ki jo sestavlja transpozicija in cikel.

Zgled 3.49. Spomnimo se, da se grupa, ki je generirana z enim samim elementom, imenuje *ciklična grupa*.

Zgled 3.50. Na množice generatorjev bi po eni strani lahko gledali podobno kot gledamo na bazo vektorskega prostora. Ta intuicija ni napačna, ampak ni povsem prava. Grupa $\mathbb{Z}$ je lahko generirana z enim elementom: $S_1 = \{1\}$. Lahko pa tvorimo večjo in odvečno množico $S_2 = \{1, 2\}$, ki je prav tako množica generatorjev grupe $\mathbb{Z}$. To množico lahko skrčimo, da tvori minimalno množico generatorjev, prav tako kot lahko skrčimo množico vektorjev, ki napenja vektorski prostor, do baze tega vektorskega prostora. Vendar pa obstajajo tudi druge množice generatorjev grupe $\mathbb{Z}$, na primer $\{2, 3\}$, ki pa jih ne moremo narediti manjše le z odstanitvijo enega elementa.

Zgled 3.51. Vsak element diedrske grupe D_n je določen s tem, kam pošlje dve sosednji oglišči ustreznega pravilnega n-kotnika. To dejstvo uporabimo tudi, ko želimo pokazati, da je grupa D_n generirana z rotacijo in zrcaljenjem.

Naj bosta v_1 in v_2 sosednji vozlišči pravilnega n-kotnika, kot je to prikazano na sliki 14a za pravilni šestkotnik.



(a) Šestkotnik in zrcaljenje ϕ. (b) Šestkotnik ter zrcaljenji ϕ in ψ.

Slika 14: Pravilni šestkotnik z označenima vozliščema v_1, v_2 in z zrcaljenjema ϕ, ψ.

Potem naj bo g nek element grupe D_n. Element g slika v_1 v vozlišče $g(v_1)$ in v_2 v vozlišče $g(v_2)$. Naj bo ρ rotacija za kot $\frac{2\pi}{n}$ v smeri urinega kazalca ali v nasprotni smeri, kakor se odločimo. Naj bo ϕ zrcaljenje, ki fiksira v_1. Potem obstaja tako nenegativno celo število m, da je $\rho^m(v_1) = g(v_1)$. Če se zgodi, da je tudi $\rho^m(v_2) = g(v_2)$, potem smo našli generator, saj je $g = \rho^m$. Povedano drugače: ker $g^{-1}\rho^m$ fiksira vozlišči v_1 in v_2, je $g^{-1}\rho^m = \mathrm{id}$, iz česar sledi, da je $\rho^m = g$. Če se slednje ne zgodi, potem element $\rho^m \cdot \phi$ pošlje $v_1 \to g(v_1)$ in $v_2 \to g(v_2)$. Zatorej je $g^{-1}\rho^m\phi = \mathrm{id}$ in posledično velja $\rho^m\phi = g$. Ker je bil g poljuben element v grupi D_n, smo pokazali, da je lahko vsak element diedrske grupe D_n predstavljen kot produkt rotacij ρ in zrcaljenja ϕ. Torej smo našli množico generatorjev $\{\rho, \phi\}$ grupe D_n.

Diedrsko grupo D_n lahko generiramo tudi z dvema sosednjima zrcaljenjema. Naj bo ϕ takšno zrcaljenje kot prej in naj bo ψ zrcaljenje n-kotnika, ki s ϕ tvori kot $\frac{\pi}{n}$, kar je za pravilni šestkotnik prikazano na sliki 14b. Potem je $\phi \cdot \psi$ rotacija za kot $\frac{2\pi}{n}$. Če sedaj uporabimo zgornji argument, potem ϕ in produkt $\phi \cdot \psi$ generirata diedrsko grupo D_n in posledično je tudi $\{\phi, \psi\}$ množica generatorjev za D_n.

Ti zgledi nam nakažejo, da ima lahko dana grupa zelo različne in zanimive množice generatorjev. Zato se ponavadi ni dobro omejiti le na eno množico generatorjev. Za konec si oglejmo še zgled grupe, ki nima končne množice generatorjev.

Zgled 3.52. Dokažimo, da grupa $(\mathbb{Q}, +)$ ni končno generirana. V ta namen predpostavimo nasprotno: naj bo $\mathbb{Q}$ končno generirana z množico $S = \{\frac{n_1}{d_1}, \frac{n_2}{d_2}, ..., \frac{n_k}{d_k}\}$. Če je d najmanjši skupni večkratnik števil $d_1, d_2, ..., d_k$, potem vsak element, ki ga lahko zapišemo kot vsoto omenjenih generatorjev in njihovih inverzov, lahko predstavimo kot $\frac{n}{d}$ za nek $n \in \mathbb{Z}$. Ampak vsak element v $\mathbb{Q}$ pa ne moremo zapisati na tak način.

3.6 Cayleyjevi grafi

Definicijo Cayleyjevih grafov je predstavil Arthur Cayley leta 1878, da bi z njihovo pomočjo pojasnil koncept abstraktnih grup, generiranih z določeno množico generatorjev. Ta definicija je nekako združila dve veji v matematiki - teorijo grup in teorijo grafov. Tako je nastala algebraična teorija grafov, v kateri se za reševanje problemov v teoriji grafov uporabijo algebraične metode. Znotraj te algebraične teorije grafov, ki se je razvila v obsežno vejo matematike, se Cayleyjevi grafi izkažejo za zelo uporabne, saj rešujejo številne praktične probleme in tudi nekatere probleme v klasični matematiki.

Ogledali si bomo nadgrajeni Cayleyjev osnovni izrek, s pomočjo katerega bomo vpeljali pojem Cayleyjevih grafov in na grupe pogledali še s kombinatoričnega vidika. Razdelek Cayleyjevi grafi je povzet po knjigah [8], [9], [10] ter zapiskov [4].

Za začetek omenimo, da v teoriji grafov nekemu grafu Γ rečemo, da je lokalno končen, če ima vsako vozlišče grafa Γ končno mnogo sosedov. Spomnimo se, da je usmerjen graf povezan, če je njegov temeljni, neusmerjen graf povezan.

Izrek 3.53 (Nadgradnja Cayleyjevega osnovnega izreka)**.** *Vsako končno generirano grupo lahko vložimo v grupo simetrij povezanega, usmerjenega, lokalno končnega grafa.*

Dokaz: Sprva je težko videti, kako bi se lotili dokazovanja zgornjega izreka. Imamo grupo G in končno množico generatorjev S, ki generira omenjeno grupo. Iz tega pa moramo dobiti tako graf kot tudi neko delovanje grupe na ta graf.

Za začetek se s pomočjo grupe G in množice generatorjev S lotimo konstrukcije grafa $\Gamma_{G,S}$. Naj bodo vozlišča grafa $\Gamma_{G,S}$ kar elementi grupe G. Sedaj pa tvorimo še za vsak $g \in G$ in vsak $s \in S$ usmerjeno povezavo, ki bo za začetno vozlišče imela element g in za končno vozlišče $g \cdot s$. Opazimo lahko, da so povezave grafa $\Gamma_{G,S}$ v korespondenci z desnim množenjem z elementi množice generatorjev S.

Da bi dokazali, da je graf $\Gamma_{G,S}$ povezan, zadošča pokazati, da lahko pridemo z vozlišča, ki je v korespondenci z elementom e, ki predstavlja enoto v grupi G, do kateregakoli drugega vozlišča g. Ker je S množica generatorjev grupe G, lahko $g \in G$ zapišemo kot produkt generatorjev in njihovih inverzov, torej $g = s_1 s_2 ... s_n$, kjer je vsak s_i v S ali v S^{-1}. Potemtakem v grafu $\Gamma_{G,S}$ obstaja naslednja pot:

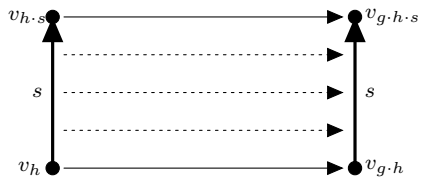
$$\underset{e}{\bullet} \xrightarrow{s_1} \underset{s_1}{\bullet} \xrightarrow{s_2} \underset{s_1 s_2}{\bullet} \xrightarrow{s_3} \ldots \xrightarrow{s_n} \underset{s_1 s_2 ... s_n = g}{\bullet}$$

Pri risanju zgornje poti smo bili malo površni, saj smo zanemarili usmerjenost posameznih povezav oziroma smo privzeli enako usmerjenost vseh povezav. Če je katera izmed s_i v izrazu $g = s_1 s_2 ... s_n$ inverzni element elementa v množici generatorjev S, potem bi potovali v nasprotno smer kot usmerjena povezava, ki povezuje $s_1 s_2 ... s_{i-1}$ z $s_1 s_2 ... s_{i-1} s_i$. Torej smo našli pot med vozliščem e in pa poljubnim vozliščem g, kar pa zadošča za dokaz povezanosti grafa $\Gamma_{G,S}$.

Da se izognemo morebitni zmedi med elementi grupe G in vozlišči grafa $\Gamma_{G,S}$, označimo vozlišča grafa $\Gamma_{G,S}$, ki so v povezavi z elementom $g \in G$, z v_g.

Graf $\Gamma_{G,S}$ je lokalno končen, ker je množica generatorjev S končna. V bistvu je vsako vozlišče vsebovano v natanko $2 \cdot |S|$ povezavah. Vozlišče v_g je začetno vozlišče natanko ene usmerjene povezave z oznako s za vsak $s \in S$, ki gre od v_g do $v_{g \cdot s}$ in v_g je končno vozlišče natanko ene usmerjene povezave, ki ima oznako s in gre od $v_{g \cdot s^{-1}}$ do v_g, za vsak $s \in S$.

Dokaz Cayleyjevega osnovnega izreka (izrek 3.10) opisuje levo delovanje grupe G na vozlišča našega grafa, kjer element $g \in G$ pošlje vozlišče v_h v vozlišče $v_{g \cdot h}$. To delovanje se lahko prenese tudi na delovanje grupe G na povezave v grafu $\Gamma_{G,S}$. Opazimo lahko, da je vozlišče v_h povezano z vozliščem $v_{h \cdot s}$ z usmerjeno povezavo s. Element $g \in G$ pošlje vozlišče v_h v vozlišče $v_{g \cdot h}$ in vozlišče $v_{h \cdot s}$ v vozlišče $v_{g \cdot h \cdot s}$. Zato lahko delovanje elementa $g \in G$ na povezave grafa $\Gamma_{G,S}$ definiramo tako, da rečemo: povezava s, ki povezuje v_h z $v_{h \cdot s}$, se prenese na povezavo s, ki povezuje $v_{g \cdot h}$ in $v_{g \cdot h \cdot s}$. Slednje je prikazano na sliki 15. ∎



Slika 15: Delovanje elementa $g \in G$ na vozlišča grafa $\Gamma_{G,S}$ se razširi na delovanje g na povezave tega grafa.

Povzemimo, kar smo odkrili v dokazu izreka 3.53, v definicijo *Cayleyjevih digrafov*. Z besedo digraf praviloma označimo usmerjen graf.

Definicija 3.54. Naj bo G grupa in $S \subset G$ množica generatorjev grupe G. Potem je *Cayleyjev digraf* grupe G glede na množico generatorjev S usmerjen graf $\Gamma_{G,S}$, katerega

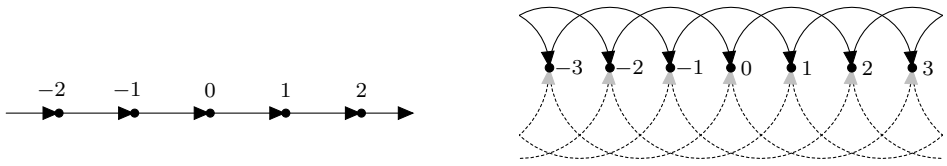
- množica vozlišč grafa $\Gamma_{G,S}$ je enaka množici elementov v grupi G;
- množica povezav grafa $\Gamma_{G,S}$ je množica urejenih parov $\{(g, g \cdot s) \mid g \in G,\ s \in S \setminus \{e\}\}$.

V dokazu nadgrajenega Caylejevega izreka opazimo, da konstrukcija delovanja grupe G na Cayleyjev digraf $\Gamma_{G,S}$ privede do takšnega delovanja, ki ohranja smeri in oznake usmerjenih povezav. Zatorej je grupa G podgrupa grupe $\mathrm{Sym}^+(\Gamma_{G,S})$.

Opomba 3.55. Arthur Cayley je predstavil Cayleyjeve digrafe v članku leta 1878. V članku med drugim omeni tudi to, da pri risanju Cayleyjevih digrafov potrebujemo različne barve, kadar imamo opravka z dvema ali več generatorji. Njegov nasvet je bil, da povezave, ki pripadajo določenemu generatorju, pobarvamo z enako barvo. Večkrat se izkaže za zelo koristno, če se držimo tega barvnega dogovora.

3.6.1 Osnovni primeri Cayleyjevih digrafov

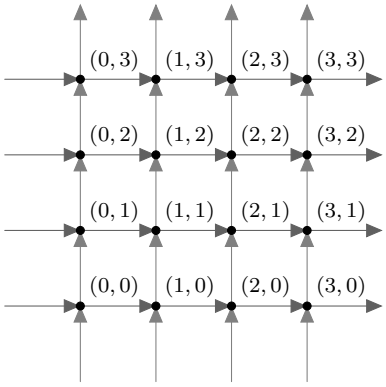
Cayleyjeva digrafa aditivne grupe $\mathbb{Z}$ glede na množici generatorjev $\{1\}$ in $\{2,3\}$ sta prikazani spodaj na sliki 16.



(a) $\Gamma_{(\mathbb{Z},+),\{1\}}$ (b) $\Gamma_{(\mathbb{Z},+),\{2,3\}}$

Slika 16: Cayleyjeva digrafa aditivne grupe $\mathbb{Z}$.

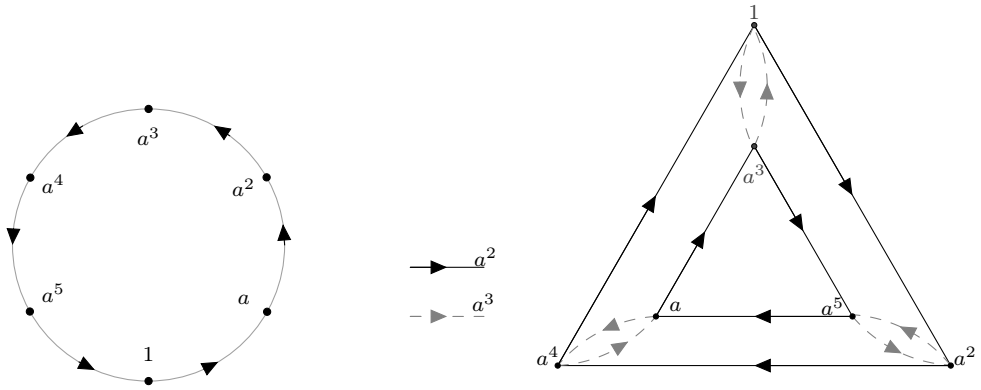
Cayleyjev digraf grupe $(\mathbb{Z}^2,+)$ glede na množico generatorjev $S=\{(1,0),(0,1)\}$ izgleda kot celoštevilska mreža v $\mathbb{R}^2$, kar lahko vidimo na sliki 17.



Slika 17: Cayleyjev digraf $\Gamma_{(\mathbb{Z}^2,+),\{(1,0),(0,1)\}}$.

Idejo o tem, kako bi izgledal Cayleyjev digraf grupe $\mathbb{Z}_n$ glede na množico generatorjev $S=\{a\}$, dobimo s pomočjo konkretnega primera za grupo $\mathbb{Z}_6$. Le-ta je narisan na sliki 18a.

Če za grupo G vzamemo aditivno grupo Z_{nm}, kjer sta m in n tuji si pozitivni celi števili, ter za množico generatorjev $S=\{a^m,a^n\}$, obenem pa grupo G generira element a, potem Cayleyjev digraf $\Gamma_{G,S}$ izgleda kot na sliki 18b.



(a) $\Gamma_{\mathbb{Z}_6,\{a\}}$ (b) $\Gamma_{\mathbb{Z}_6,\{a^2,a^3\}}$

Slika 18: Cayleyjeva digrafa grupe $\mathbb{Z}_6$ glede na množici generatorjev $\{a\}$ in $\{a^2, a^3\}$.

3.6.2 Osnovne lastnosti Cayleyjevih digrafov in grafov

Sledenje elementom po poteh v Cayleyjevem digrafu se ujema s produktom generatorjev v grupi, katere množica generatorjev in sama grupa tvorita omenjeni Cayleyjev digraf.

Naj bo G grupa in S množica generatorjev grupe G. V dokazu 3.53 smo pokazali, da je končna pot povezav v digrafu $\Gamma_{G,S}$ končen niz povezav v digrafu $\Gamma_{G,S}$, kjer lahko sledimo povezavi po njeni usmerjenosti ali v nasprotno smer tako, da je končno vozlišče vsake povezave v nizu tudi začetno vozlišče naslednje povezave, ki se nahaja v nizu. Digraf Γ je povezan, če za vsaki dve vozlišči obstaja pot povezav, ki ima eno od teh vozlišč za začetno in drugo za končno vozlišče. Niz oznak na povezavah končne poti je niz elementov iz $S \cup S^{-1}$, kjer je i-ti element v nizu oznak oznaka na i-ti povezavi v poti povezav, lahko pa se zgodi, da je ta oznaka invertirana, če potujemo v nasprotno smer od usmerjenosti te povezave.

Naslednjo lemo smo v resnici dokazali že v dokazu nadgrajenega Cayleyjevega izreka.

Lema 3.56. *V digrafu $\Gamma_{G,S}$ obstaja pot iz vozlišča e, ki je nevtralni element v grupi G, do vozlišča $g \in G$ z nizom oznak $s_1^{k_1}$, $s_2^{k_2}$, ..., $s_n^{k_n}$, kjer so $s_i \in S$ in $k_i \in \{-1, 1\}$, če in samo če velja naslednja enakost:*

$$g = s_1^{k_1} s_2^{k_2} ... s_n^{k_n}.$$

Trditev 3.57. *Naj bo G grupa z množico generatorjev S in naj bo $\Gamma_{G,S}$ Cayleyjev digraf grupe G glede na S. Potem ima vsako vozlišče grafa $\Gamma_{G,S}$ natanko eno povezavo s posamezno oznako iz množice S, ki ima to vozlišče za začetno vozlišče, in natanko eno povezavo s posamezno oznako iz množice S, ki ima omenjeno vozlišče za končno vozlišče. Velja tudi, da je digraf $\Gamma_{G,S}$ povezan.*

Dokaz: Za vsak element $g \in G$ in vsak $s \in S$ obstaja natanko en element $h_1 \in G$, za katerega velja $h_1 = gs$, in obstaja natanko en element $h_2 \in G$, za katerega je $g = h_2 s$. To velja, ker je v grupi možno pravilo krajšanja. Zgornje pa pomeni, da obstaja natanko ena povezava digrafa z oznako s, ki vozlišče g zapušča (poteka od g do $gs = h_1$) in natanko ena povezava z oznako s, ki se konča v vozlišču g (potuje od $h_2 = gs^{-1}$ do g).

Pokažimo še, da je digraf $\Gamma_{G,S}$ povezan. Ker elementi S generirajo grupo G, potem za vsak $g \in G$ obstaja izraz za g kot produkt elementov množice S in njihovih inverzov. Potem po lemi 3.56 obstaja pot iz vozlišča e do vozlišča g. Da dobimo pot iz vozlišča g do vozlišča h, združimo pot iz g v e in pot iz e v h. Ker med poljubnima dvema vozliščema obstaja pot, je digraf povezan. ∎

Trditev 3.58. *Naj bo dan Cayleyjev digraf $\Gamma_{G,S}$ grupe G glede na množico generatorjev S. Potem lahko rekonstruiramo operacijo na grupi G.*

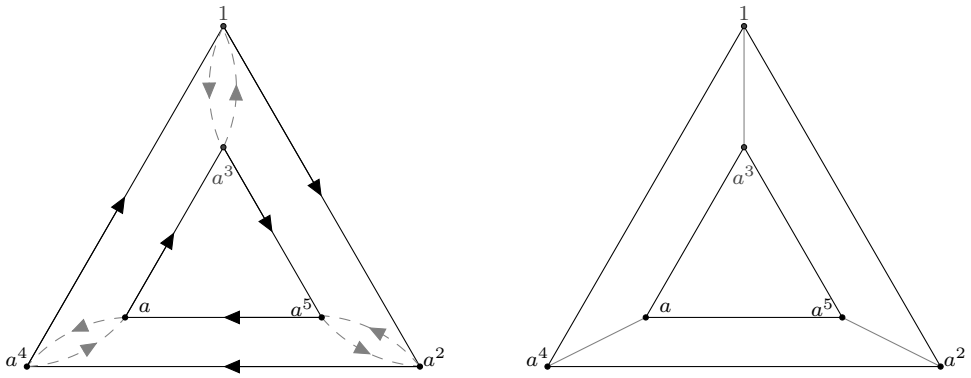
Dokaz: Množica elementov grupe G je množica vozlišč grafa $\Gamma_{G,S}$, zato vemo, kakšna je grupa G kot množica. Naj bosta $g, h \in G$. Ker je $\Gamma_{G,S}$ povezan, obstaja pot iz vozlišča e v vozlišče g in pot iz vozlišča e v vozlišče h, kjer je e enota v grupi G. Po lemi 3.56 ti dve poti za elementa g in h podata izraza v obliki produkta generatorjev in njihovih inverzov. Izraza za g in h pomnožimo, da dobimo izraz za $g \cdot h$. Po omenjeni lemi nam dobljeni izraz poda pot iz vozlišča e do vozlišča $g \cdot h$. To nam omogoča, da opredelimo vozlišče za $g \cdot h$ s pomočjo vozlišč g in h. Torej lahko res rekonstruiramo operacijo v grupi G. ∎

Vpeljimo dve dodatni zahtevi na Cayleyjevih digrafih, in sicer najprej zahtevo, da množica generatorjev S ne vsebuje nevtralnega elementa grupe G, torej $e \notin S$. S tem smo se izognili obstoju zank v digrafu. Druga zahteva pa je, da naj bo množica generatorjev S *simetrična* ali *zaprta za inverze*. Množica S je simetrična, če dejstvo $s \in S$ implicira, da je tudi $s^{-1} \in S$. Ta pogoj lahko zapišemo tudi kot $S = S^{-1}$, kjer je $S^{-1} := \{s^{-1} \mid s \in S\}$. S to dodatno zahtevo na Cayleyjevih digrafih smo dosegli, da če se v grafu nahaja povezava iz vozlišča g do vozlišča $g \cdot s$, imamo v tem grafu tudi povezavo iz vozlišča $g \cdot s$ v vozlišče $(g \cdot s) \cdot s^{-1} = g$. Razlog za vpeljavo druge zahteve je ta, da je povezava v grafu ne glede na to, katero vozlišče je mišljeno kot končno. Tako lahko zanemarimo usmerjenost povezav v Cayleyjevem digrafu in dve usmerjeni povezavi združimo v eno neusmerjeno. Torej lahko Cayleyjev digraf obravnavamo kot neusmerjenega, zato tovrsten graf poimenujemo kar Cayleyjev graf.

Definicija 3.59. Naj bo G grupa in $S \subset G$ množica generatorjev grupe G. Potem je *Cayleyjev graf* grupe G glede na množico generatorjev S neusmerjen graf $\Gamma_{G,S}$, katerega

- množica vozlišč grafa $\Gamma_{G,S}$ je enaka množici elementov v grupi G;
- množica povezav grafa $\Gamma_{G,S}$ je množica neurejenih parov $\{\{g, g \cdot s\} \mid g \in G,\ s \in S \setminus \{e\}\}$.

Oglejmo si razliko med Cayleyjevimi digrafi in Cayleyjevimi grafi na primeru grupe $\mathbb{Z}_6$ z množico generatorjev $S = \{a^2, a^3\}$. Cayleyjev digraf $\Gamma_{\mathbb{Z}_6,S}$ je prikazan na sliki 19a. Z dodatnima zahtevama na tem Cayleyjevem digrafu dobimo Cayleyjev graf, ki je prikazan na sliki 19b. Le-ta je neusmerjen in vsak par vzporednih, nasprotno usmerjenih povezav v Cayleyjevem digrafu smo nadomestili z eno neusmerjeno povezavo.



(a) Cayleyjev digraf $\Gamma_{\mathbb{Z}_6,\{a^2,a^3\}}$. (b) Cayleyjev graf $\Gamma_{\mathbb{Z}_6,\{a^2,a^3\}}$.

Slika 19: Cayleyjev digraf in graf grupe $\mathbb{Z}_6$ glede na množico generatorjev $\{a^2, a^3\}$.

Razlika med Cayleyjevim digrafom in Cayleyjevim grafom je tudi ta, da ima usmerjen digraf stopnjo vozlišč vedno enako $2n$, kjer je n število generatorjev dane grupe, neusmerjen graf pa ne, če je kateri od generatorjev grupe stopnje 2.

V nadaljevanju magistrskega dela se bomo povečini ukvarjali z neusmerjenimi grafi, kar je bil tudi povod za vpeljavo dodatnih zahtev in s tem tudi definicije Cayleyjevih grafov. Besedi digraf in graf bosta nakazali, katero vrsto Cayleyjevih grafov bomo imeli v mislih.

Zgled 3.60. Pokažimo, da Petersenov graf ni Cayleyjev graf nobene grupe, kljub temu, da je regularen graf. Tu se nanašamo na Cayleyjev digraf z dodatno zahtevo o simetričnosti njegove množice generatorjev in ga tako lažje primerjamo z neusmerjenim Petersenovem grafom. Pri dokazu bomo potrebovali dejstvi, da Petersenov graf ne vsebuje cikla dolžine 4 ter da ni dvodelni graf.

Pa denimo, da je Petersenov graf P Cayleyjev graf $\Gamma_{G,S}$ grupe G za simetrično množico generatorjev S. Ker je Petersenov graf P 3-regularen z desetimi vozlišči, je moč grupe G enaka 10 in moč množice S enaka 3. Obstajata le dve neizmorfni grupi reda 10, to sta ciklična grupa $\mathbb{Z}_{10}$ in diedrska grupa D_5. Utemeljitev tega lahko preberemo v knjigi [5, str. 93,94]. Torej je grupa G z močjo 10, izomorfna grupi $\mathbb{Z}_{10}$ ali grupi D_5. Zaradi pogoja simetričnosti množice generatorjev S za grupo G, le-ta sestoji iz treh elementov reda 2 ali pa iz enega elementa reda 2, enega elementa reda več kot 2 in njegovega inverza. Zato ločimo primere:

1. Naj bo $G \cong \mathbb{Z}_{10}$. Ker ta ciklična grupa vsebuje le en element reda 2, to je element 5, je množica $S = \{5, x, -x\}$, kjer je $x \notin \{0, 5\}$. Vendar pa je potem $(0, 5, x + 5, 5, 0)$ cikel dolžine 4 v Petersenovem grafu P. Tako smo prišli do protislovja, saj je najmanjši cikel v Petersenovem grafu P dolžine 5.

2. Naj bo grupa $G \cong D_5 = \{r, s \mid s^2 = r^5 = \mathrm{id},\ srs = r^{-1}\}$, kjer sta rotacija r in zrcaljenje s enaki kot v zgledu 2.10. Potem so elementi reda 2 v grupi G natanko elementi iz množice $\{s, sr, sr^2, sr^3, sr^4\}$. Ker ima množica S enega ali tri elemente reda 2, obravnavamo dve možnosti:

   2.1. Naj bo množica $S = \{sr^a, sr^b, sr^{-b}\}$, kjer je $a \in \{0, 1, 2, 3, 4\}$ in $b \in \{1, 2\}$. V tem primeru je $(\mathrm{id}, rs^a, r^{a-b}s, r^{-b}, \mathrm{id})$ cikel dolžine 4 v Petersenovem grafu in smo spet prišli do protislovja.

   2.2. Naj bo množica $S = \{sr, sr^b, sr^c\}$, kjer so $a, b, c \in \{0, 1, 2, 3, 4\}$. Če naredimo particijo elementov grupe D_5 na množici $\{\mathrm{id}, r, r^2, r^3, r^4\}$ in $\{s, sr, sr^2, sr^3, sr^4\}$, lahko hitro preverimo, da je pripadajoči Cayleyjev graf dvodelni. Spet smo prišli do protislovja, saj Petersenov graf P ni dvodelen.

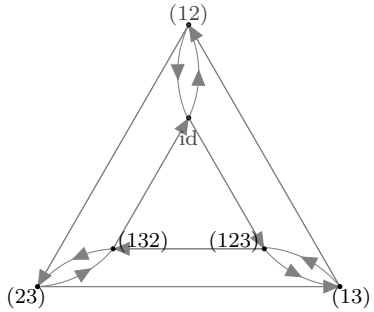
V vseh primerih smo naleteli na protislovje, zato lahko zaključimo, da Petersenov graf ni Cayleyjev graf za nobeno grupo G.

3.6.3 Cayleyjevi digrafi ter grafi simetričnih in diedrskih grup

Najboljši način za razumevanje pojma Cayleyjevega digrafa ali grafa je ta, da preučimo nekaj netrivialnih primerov teh grafov, ki nastanejo iz značilnih družin grup.

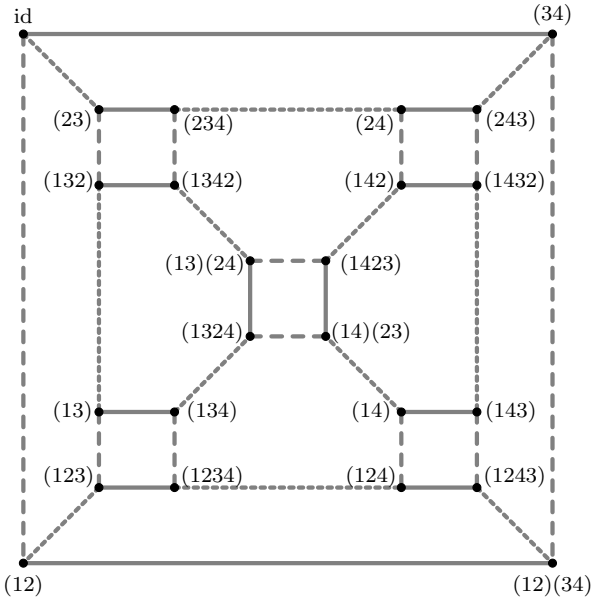
Cayleyjevi digrafi in Cayleyjevi grafi simetričnih grup

Najprej si oglejmo Cayleyjev digraf simetrične grupe S_3 z množico generatorjev $S = \{(12), (123)\}$. Le-ta ima šest vozlišč, ki so elementi simetrične grupe $S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$, povezave Cayleyjevega digrafa pa razberemo iz množice $\{(g, g \cdot s) \mid g \in S_3,\ s \in \{(12), (123)\}\}$. Tako nastane digraf na sliki 20.



Slika 20: Cayleyjev digraf $\Gamma_{S_3,\{(12),(123)\}}$.

Zdaj pa si oglejmo še Cayleyjev graf simetrične grupe štirih elementov S_4 z množico generatorjev $S = \{(12), (23), (34)\}$. Ker je moč grupe S_4 enaka 24, bo imel Cayleyjev graf 24 vozlišč. Ker je moč množice generatorjev enaka 3, bo vsako vozlišče vsebovano v treh povezavah. Produkta $(12)(23) = (123)$ in $(23)(34) = (234)$ sta oba reda 3, transpoziciji (12) in (34) pa komutirata. Iz tega sledi, da bo vsako vozlišče, ki je del povezav, ki predstavljajo (12) in (23), določalo 6-cikel, povezave, ki predstavljajo (23) in (34), določajo še en 6-cikel, medtem ko povezave, ki so v korespondenci z (12) in (34), tvorijo 4-cikel. Posledično lahko pri vsakem vozlišču tega Cayleyjevega grafa, razen pri skrajno zunanjih vozliščih, vidimo dva šestkotnika in en kvadrat. Pridobili smo dovolj podatkov, da določimo obliko Cayleyjevega grafa $\Gamma_{S_4,\{(12),(23),(34)\}}$. Le-ta je prikazan sliki 21.

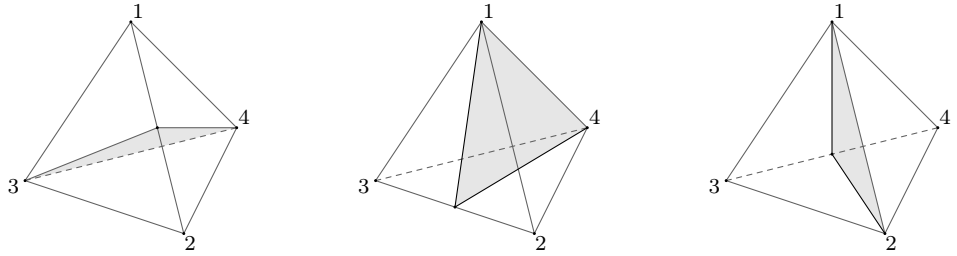


Slika 21: Cayleyjev graf $\Gamma_{S_4,\{(12),(23)(34)\}}$.

Kdor je bolj domač na področju Arhimedskih teles, je verjetno opazil, da ta Cayleyjev graf izgleda kot robovi prisekanega oktaedra. To ni naključje. Najprej predstavimo grupo S_4 kot grupo simetrij tetraedra $\mathbb{T}$. Tega se lotimo tako, da najprej identificiramo štiri oglišča tetraedra $\mathbb{T}$ s števili v množici $[4] = \{1, 2, 3, 4\}$. Dejstvo, da vsaka simetrija tetraedra $\mathbb{T}$ povzroči neko permutacijo množice $[4]$, nam da idejo za konstrukcijo homomorfizma $\phi\colon \mathrm{Sym}(\mathbb{T}) \to S_4$.

Za začetek pokažimo, da je homomorfizem ϕ surjektiven. Za surjektivnost je dovolj pokazati, da so vse tri transpozicije $(12), (23), (34)$ v sliki homomorfizma ϕ. Zrcaljenje preko ravnine, razpete preko robu tetraedra, ki povezuje oglišči 3 in 4, in skozi razpolovišča robu, ki povezuje oglišči 1 in 2, nas s homomorfizmom ϕ privede do transpozicije (12). Analogna zrcaljenja porodijo množico generatorjev

$S = \{(12), (23), (34)\}$ za grupo S_4. Ravnine, preko katerih zrcalimo in so osnova za pridobitev transpozicij v množici S preko homomorfizma ϕ, so prikazane na sliki 22.



(a) Zrcaljenje, ki nas pripelje do transpozicije (12).

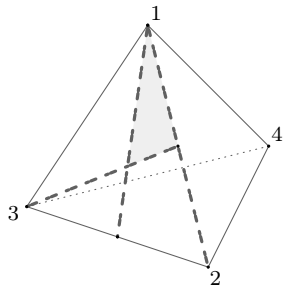
(b) Zrcaljenje, ki vodi do transpozicije (23).

(c) Zrcaljenje, ki ustreza transpoziciji (34).

Slika 22: Zrcaljenja, s pomočjo katerih preko homomorfizma ϕ pridemo do transpozicij $\{(12), (23), (34)\}$, kar pa je ravno naša množica generatorjev za grupo S_4.

Ker imata obe grupi, ki nastopata v homomorfizmu ϕ, moč 24 ter je ϕ surjektiven, mora veljati, da je naš homomorfizem ϕ izomorfizem.

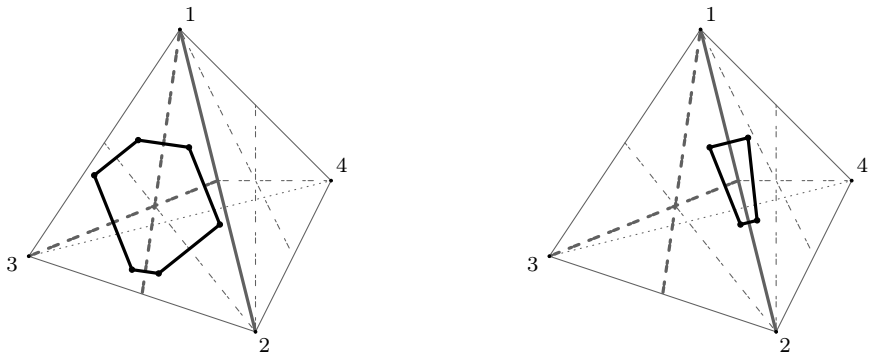
Sedaj želimo narisati še Cayleyjev graf grupe S_4 glede na množico generatorjev $S = \{(12), (23), (34)\}$, v ta namen pa moramo najprej poiskati točko v tetraedru $\mathbb{T}$, ki ima trivialen stabilizator. Za začetek si narišimo nekaj množic negibnih točk za zrcaljenja, ki so v korespondenci s transpozicijami $\{(12), (23), (34)\}$. Dobili smo območje trikotne oblike na zunanjosti tetraedra, le-tega lahko uzremo na sliki 23, ki ustreza pogoju, da imajo vse točke znotraj tega območja trivialen stabilizator.



Slika 23: Deli množic negibnih točk za zrcaljenja, ki predstavljajo transpozicije (12), (23) in (34), so na sliki označeni s črtkanimi črtami. Pojavi se tudi trikotno območje na zunanji ploskvi tetraedra, znotraj katerega se nahajajo točke s trivialnim stabilizatorjem.

Znotraj tega območja si nato izberemo poljubno točko in na njej uporabimo zrcaljenji v korespondenci s transpozicijama (12) in (23). Tako dobimo prvi šestkotnik

našega Cayleyjevega grafa. Zdaj na isti točki uporabimo še zrcaljenji, ki predstavljata transpoziciji (12) in (34), in na tetraedru zagledamo del pravokotne oblike, ki nastopa v Cayleyjevem grafu. To si oglejmo na sliki 24. Šestkotnik, ki nastane z zrcaljenjema, ki sta v korespondenci s transpozicijama (23) in (34), se nahaja pod vozliščem 1, zaradi nepreglednosti slike ga ne predstavimo posebej.



Slika 24: Dva dela Cayleyjevega grafa $\Gamma_{S_4,\{(12),(23),(34)\}}$ - eden od dveh šestkotnikov in pravokotnik - sta označena odebeljeno na posameznih ploskvah tetraedra.

Vidimo torej lahko, da osnovna struktura našega Cayleyjevega grafa izhaja iz robov Arhimedskega telesa.

Opomba 3.61. Opišimo pogosto tehniko za odkrivanje strukture Cayleyjevega grafa, ki smo jo uporabili tudi na zgornjem zgledu. Začeli smo z delovanjem grupe G, katere Cayleyjev graf nas zanima, na nek geometrijski objekt. Zgoraj je bila to grupa S_4, ki je delovala na tetraeder. Potem smo poiskali točko v prostoru, ki se je z delovanjem grupe gibala prosto oziroma je imela trivialen stabilizator. Po posledici 3.27 sledi, da obstaja bijekcija med orbito te točke pod delovanjem grupe G in med elementi grupe G. Zato lahko za množico vozlišč Cayleyjevega grafa uporabimo orbito te točke. V zgornjem primeru je bila naša točka premišljeno izbrana, da so bile povezave grafa lepo razporejene po prostoru.

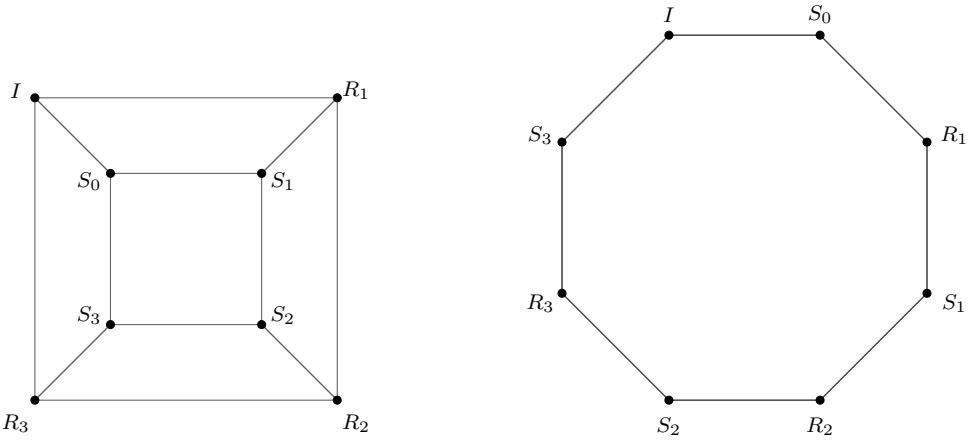
Cayleyjevi grafi diedrskih grup

Naj bo D_n diedrska grupa reda $2n$. Kot smo razpravljali v zgledu 3.51, imamo dve značilni množici generatorjev za diedrsko grupo D_n: $H_1 = \{$zrcaljenje $\phi = S_0$, rotacija $\rho = R_1$ za kot $\frac{2\pi}{n}\}$ ter $H_2 = \{$zrcaljenji $\phi = S_0$, $\psi = S_3\}$, za kateri velja, da je kot med premicama, ki tvorita ti dve zrcaljenji, enak $\frac{\pi}{n}$. Poglejmo si Cayleyjeva grafa za diedrsko grupo D_4 glede na množico generatorjev H_1 in H_2. Množica vozlišč Cayleyjevih grafov bo enaka množici elementov v diedrski grupi D_4,

$\{I = R_0, R_1, R_2, R_3, S_0, S_1, S_2, S_3\}$, torej bo njena moč enaka 8. Množici povezav pa se zaradi različnih množic generatorjev precej razlikujeta:

- Če začnemo s prvo množico generatorjev H_1 diedrske grupe D_4, dobimo za množico povezav naslednjo množico $\{\{I, S_0\}, \{I, R_1\}, \{R_1, S_1\}, \{R_1, R_2\}, \{R_2, S_2\}, \{R_2, R_3\}, \{R_3, S_3\}, \{R_3, I\}, \{S_0, S_3\}, \{S_1, S_0\}, \{S_2, S_1\}, \{S_3, S_2\}\}$.
- Če zberemo vse povezave Cayleyjevega grafa, ki nastanejo s pomočjo druge množice generatorjev H_2, dobimo naslednjo množico povezav $\{\{I, S_0\}, \{I, S_3\}, \{R_1, S_1\}, \{R_1, S_0\}, \{R_2, S_2\}, \{R_2, S_1\}, \{R_3, S_3\}, \{R_3, S_2\}\}$.

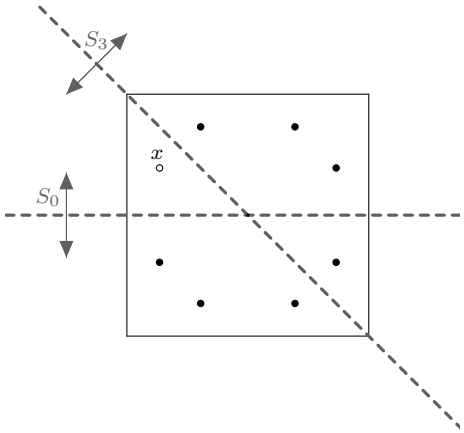
Cayleyjeva grafa diedrske grupe D_4 glede na množici generatorjev H_1 in H_2 sta narisana na sliki 25.



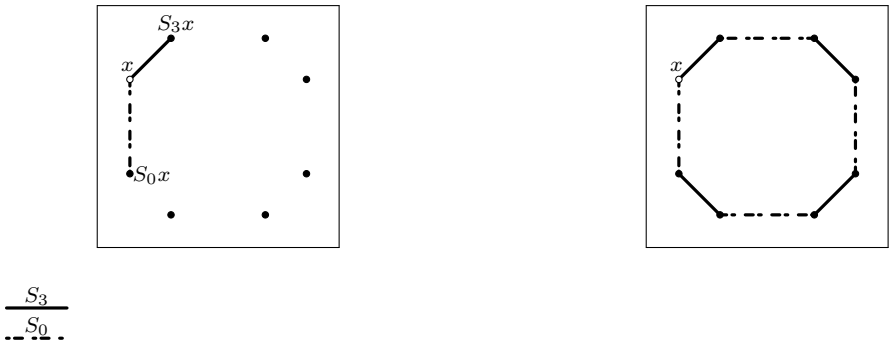
(a) Γ_{D_4,H_1} (b) Γ_{D_4,H_2}

Slika 25: Cayleyjeva grafa diedrske grupe D_4 glede na množici generatorjev H_1, H_2.

Ta Cayleyjeva grafa pa lahko podobno, kot smo to storili v primeru simetričnih grup, skonstruiramo direktno iz delovanja diedrske grupe D_n na pravilni n-kotnik. Oglejmo si to na primeru diedrske grupe D_4 in množice generatorjev H_2. Na kvadratu si izberimo točko x, ki ima trivialen stabilizator. Posledično so elementi v orbiti točke x v korespondenci z osmimi elementi diedrske grupe D_4. Na sliki 26 sta označeni še zrcaljenji S_0 in S_3, ki sta v množici generatorjev H_2 grupe D_4. Sedaj lahko povežemo točke v orbiti tako, da tvorijo Cayleyjev graf glede na označena generatorja. Začnimo z našo začetno točko x in potem na njej uporabimo generatorja S_0 in S_3. To je prikazano na levi strani slike 27. Po definiciji Cayleyjevega grafa je točka S_3x povezana z vozliščem S_0S_3x, to pa je ravno rotacija v smeri urinega kazalca za kot $\frac{\pi}{2}$. Če nadaljujemo na tak način, lahko preverimo, da desna stran slike 27 res prikazuje Cayleyjev graf diedrske grupe D_4 glede na množico generatorjev H_2.



Slika 26: Diedrska grupa D_4 je generirana z zrcaljenjema S_0 in S_3.



Slika 27: Cayleyjev graf diedrske grupe D_4 glede na množico generatorjev $\{S_0, S_3\}$ lahko konstruiramo tako, da povežemo elemente v orbiti točke s trivialnim stabilizatorjem.

3.7 Fundamentalne domene in množice generatorjev

Naj bo G grupa, ki deluje na povezan graf Γ. Oglejmo si, kako tvorimo fundamentalne domene za delovanje grupe G in ko bomo razumeli sam pojem fundamentalnih domen, si bomo ogledali še, kako z njihovo pomočjo poiščemo množice generatorjev za dano grupo. Spodaj opisana tehnika je le en zgled, kako lahko razumevanje pojma delovanja grupe na nek geometrijski objekt poda informacijo o sami grupi. To poglavje je povzeto po knjigi [10].

Lema 3.62. *Če grupa G deluje na povezan graf Γ, potem obstaja takšna podmnožica $\mathcal{F} \subset \Gamma$, ki izpolnjuje naslednje pogoje:*

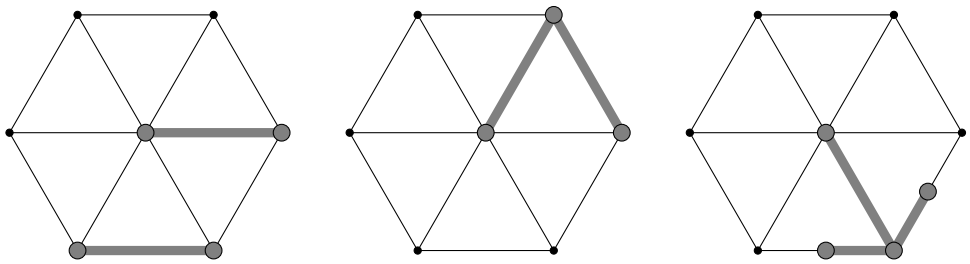
1. *$\mathcal{F}$ je zaprta;*

2. *množica $\{g \cdot \mathcal{F} \mid g \in G\}$ pokrije graf Γ;*

3. *nobena podmnožica množice $\mathcal{F}$ ne zadošča pogojema 1 in 2.*

Podmnožico $\mathcal{F}$ imenujemo fundamentalna domena za delovanje grupe G na graf Γ.

Zgled 3.63. Podan imamo graf $\Gamma = W_6$, ki mu v teoriji grafov pravijo *kolo*. Oglejmo si tri zglede fundamentalnih domen za delovanje grupe $\mathbb{Z}_6$ na graf Γ, kjer za delovanje te grupe vzamemo kar rotacije. Vsaka fundamentalna domena za delovanje $\mathbb{Z}_6 \curvearrowright \Gamma$ mora vsebovati osrednje vozlišče grafa Γ, da zadostimo drugemu pogoju v zgornji lemi. Po tem pa imamo veliko možnosti, kako bi konstruirali fundamentalno domeno. Na sliki 28 so prikazane tri možnosti.



Slika 28: Trije zgledi fundamentalnih domen za delovanje grupe $\mathbb{Z}_6$ z rotacijami na graf kolesa W_6.

V zgledu smo sestavili fundamentalno domeno tako, da smo najprej začeli z enim samim vozliščem in smo nato dodajali vozlišča in povezave grafa Γ, dokler ni bila podmnožica grafa dovolj velika, da je slika tega podgrafa po delovanju grupe G pokrila celoten graf. Sedaj pa se lotimo dokaza leme 3.62 o fundamentalni domeni.

Dokaz: Lotimo se konstrukcije fundamentalne domene in pri tem skušajmo zadostiti vsem trem pogojem, ki jih zahteva lema 3.62. Začnimo z vozliščem $v \in \Gamma$ in si zamislimo povezane podgrafe $\mathcal{C}$ v grafu Γ, za katere velja naslednje:

1. $v \in \mathcal{C}$ in

2. če sta x in y različni si vozlišči v podgrafu $\mathcal{C}$, potem ne obstaja tak element $g \in G$, da bi veljalo $g \cdot x = y$.

Samo vozlišče v zadošča zgornjima pogojema, zatorej takšni podgrafi v grafu Γ zagotovo obstajajo. Naj bo $\mathcal{C}_0 \subset \mathcal{C}_1 \subset \mathcal{C}_2 \subset ...$ zaporedje podgrafov, ki zadoščajo zgornjima pogojema in kjer je en podgraf ustrezno vsebovan v naslednjem.

Če obstaja le končno mnogo orbit vozlišč pod delovanjem grupe G na graf Γ in je graf Γ lokalno končen, potem bo eden od $\mathcal{C}_i$ v zaporedju podgrafov maksimalen podgraf, ki zadošča zgornjima dvema pogojema. Ta maksimalen podgraf bomo označili z $\mathcal{M}$.

V nasprotnem primeru pa tvorimo maksimalen podgraf, ki zadošča našima pogojema, z definicijo $\mathcal{M} = \bigcup \mathcal{C}_i$, kjer je zaporedje podgrafov $\mathcal{C}_i$ največje možno (tu se nanašamo na aksiom izbire v teoriji množic). Preverimo, ali naš novo definirani $\mathcal{M} = \bigcup \mathcal{C}_i$ zadošča prvemu in drugemu pogoju na začetku dokaza. Opazimo, da je $v \in \mathcal{C}_0 \subset \mathcal{M}$, torej zadošča prvemu pogoju. Če sta si vozlišči x in y različni v $\mathcal{M}$, potem mora obstajati nek $\mathcal{C}_i$, ki ju vsebuje, le-ta pa že zadošča pogojema 1 in 2 zgoraj. Zatorej ne obstaja $g \in G$, ki prenese x v y.

Ni nujno, da dobljeni podgraf $\mathcal{M}$ že tvori fundamentalno domeno za delovanje grupe G na graf Γ, zagotovo pa vsebuje vsa vozlišča, ki bi jih potrebovali za konstrukcijo fundamentalne domene.

Dokažimo sedaj, da slika $\mathcal{M}$ po delovanju grupe G vsebuje vsa vozlišča grafa Γ. Pa recimo ravno nasprotno: obstaja vozlišče $v_0 \in \Gamma$, ki ni vsebovano v $g \cdot \mathcal{M}$, kjer je $g \in G$. Naj bo $\{v_0, v_1, ..., v_n\}$ množica vozlišč v najkrajši poti povezav, ki povezuje vozlišče v_0 z vozliščem v $G \cdot \mathcal{M}$. Veljati mora, da vozlišče v_{n-1} ni vsebovano v $G \cdot \mathcal{M}$, saj bi sicer obstajala krajša pot do $G \cdot \mathcal{M}$. To implicira, da je vozlišče v_{n-1} izven $G \cdot \mathcal{M}$, ki je z $G \cdot \mathcal{M}$ povezano z eno samo povezavo. Zato lahko domnevamo, da je $v_0 \in \Gamma \setminus G \cdot \mathcal{M}$ in da obstaja povezava e, ki povezuje vozlišče v_0 z nekim vozliščem v $g \cdot \mathcal{M}$ za nek $g \in G$. Domnevamo torej lahko, da je vozlišče v_{n-1} kar vozlišče v_0. Toda potem bi lahko dodali v $\mathcal{M}$ še vozlišči $g^{-1} \cdot v_0$ in $g^{-1} \cdot e$, s tem pa bi ustvarili večji podgraf, ki bi zadoščal pogojema 1 in 2, to pa je v protislovju z dejstvom, da je $\mathcal{M}$ maksimalen podgraf, ki zadošča omenjenima pogojema. Torej velja, če je vozlišče $v_0 \in \Gamma$, potem je to vozlišče $v_0 \in g \cdot \mathcal{M}$ za nek $g \in G$.

Za zaključek dokaza moramo, če je to potrebno, še razširiti $\mathcal{M}$ tako, da bo slika $\mathcal{M}$ po delovanju grupe G pokrila vsako povezavo grafa Γ. Če so v grafu Γ povezave, ki niso vsebovane v $G \cdot \mathcal{M}$, potem tvorimo fundamentalno domeno $\mathcal{F}$ z dodajanjem polovičnih povezav v $\mathcal{M}$. Domnevajmo, da imamo povezavo $e \notin G \cdot \mathcal{M}$, kjer je presek množice krajišč povezave e z množico $\mathcal{M}$ neprazen. Če velja, da je množica krajišč povezave e podmnožica množice $\mathcal{M}$, potem lahko v $\mathcal{M}$ dodamo povezavo e in še vedno zadostimo pogojema. Zato lahko domnevamo, da obstaja povezava e s krajišči $\{v, w\}$, za kateri velja, da je $v \in \mathcal{M}$ in $w \notin \mathcal{M}$. Naj bo h_e zaprta polovica povezave e, ki vsebuje $v \in \mathcal{M}$. Definirajmo $\mathcal{F}$ kot unijo $\mathcal{M}$ in teh polovičnih povezav.

Ker je $\mathcal{F} \supset \mathcal{M}$, je množica vozlišč $V(\Gamma) \subset G \cdot \mathcal{F}$. Pokazati nam preostane le še, da so povezave v grafu Γ tudi v $G \cdot \mathcal{F}$. Naj bo e povezava v Γ s krajišči $\{v, w\}$. Če povezava $e \notin G \cdot \mathcal{M}$, potem obstajata taka elementa g_1 in g_2 v grupi G, da je $v \in g_1 \cdot \mathcal{M}$ in $w \in g_2 \cdot \mathcal{M}$. Posledično bo povezava e pokrita z g_1 in g_2 slikami polovičnih povezav, dodanih v $\mathcal{M}$ pri konstrukciji fundamentalne domene $\mathcal{F}$. ∎

Zgled 3.64. Za zgled, kjer $\mathcal{M}$ ne more biti sama po sebi fundamentalna domena, služijo Cayleyjevi grafi. Delovanje grupe G na njen Cayleyjev graf Γ je vozliščno

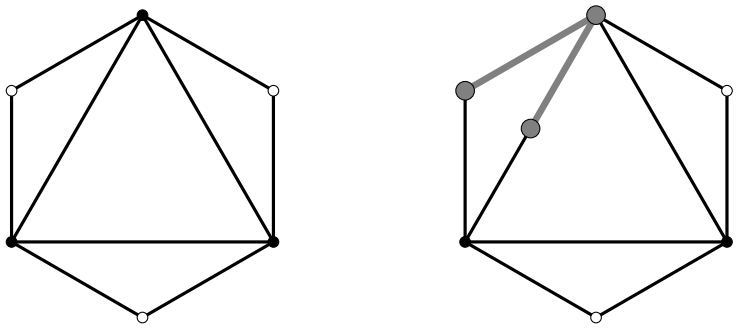
tranzitivno, saj če sta h_1, h_2 različni si vozlišči, potem je $g \cdot h_1 = h_2$, če vzamemo za $g = h_2 h_1^{-1} \in G$. Od tod sledi, da je podgraf $\mathcal{M}$ sestavljen iz enega samega vozlišča v. Torej je $G \cdot \mathcal{M}$ množica vseh vozlišč grafa Γ in $G \cdot \mathcal{M}$ ne vsebuje nobene povezave grafa Γ. V primeru delovanja grupe na njen Cayleyjev graf fundamentalna domena $\mathcal{F}$ izgleda kot zvezda, sestavljena iz enega vozlišča v in polovičnih povezav h_e, za katere velja, da povezava e vsebuje vozlišče v.

Primer 3.65. Naj bo graf Γ polni dvodelni graf $K_{m,n}$, kjer je $n \neq m$. Naj bo $G = \mathrm{Sym}(\Gamma)$. Opazimo, da G deluje tranzitivno na obeh množicah vozlišč $V_\circ$ in $V_\bullet$ grafa $K_{m,n}$. Torej lahko v $\mathcal{M}$ vzamemo katerokoli povezavo v Γ in za konstrukcijo fundamentalne domene ni potrebe, da bi dodajali še polovične povezave.

Če pa je $n = m$, potem obstaja simetrija grafa Γ, ki zamenja vozlišča množic $V_\circ$ in $V_\bullet$. V tem primeru je $\mathcal{M}$ sestavljena le iz enega vozlišča, fundamentalno domeno pa lahko tvorimo z dodajanjem tistih polovičnih povezav, ki vsebujejo to vozlišče.

Primer 3.66. Simetrijska grupa grafa Γ na sliki 29 je sestavljena iz identitete, rotacije za kot $\frac{2\pi}{3}$, rotacije za kot $\frac{4\pi}{3}$ ter treh zrcaljenj, katerih osi potekajo skozi nasprotna si črna in bela vozlišča. Hitro vidimo, da je $\mathrm{Sym}(\Gamma)$ izomorfna diedrski grupi D_3.

Ta grupa deluje tranzitivno na množico vozlišč s stopnjo 4 in na množico vozlišč s stopnjo 2. Ne obstaja pa simetrija grafa Γ, ki bi preslikala vozlišče s stopnjo 2 v vozlišče s stopnjo 4. Zato lahko $\mathcal{M}$ vsebuje vsako povezavo, ki povezuje vozlišči z različnima stopnjama. Slika te povezave po delovanju grupe $\mathrm{Sym}(\Gamma)$ je le šestkotnik, sestavljen iz zunanjih povezav, ne vsebuje pa povezav v notranjosti grafa Γ. Da bi $\mathcal{M}$ lahko tvoril fundamentalno domeno, mu je potrebno dodati še polovično povezavo. To je prikazano na desni strani slike 29.



Slika 29: Na levi je prikazan dvodelni graf Γ, ki ima dve orbiti vozlišč glede na delovanje $\mathrm{Sym}(\Gamma)$. Na desni pa je s sivo označena fundamentalna domena za $\mathrm{Sym}(\Gamma) \curvearrowright \Gamma$.

Izrek 3.67. *Naj grupa G deluje na povezan graf Γ s fundamentalno domeno $\mathcal{F}$. Potem je množica elementov*

$$S = \{g \in G \mid g \neq e \text{ in } g \cdot \mathcal{F} \cap \mathcal{F} \neq \emptyset\}$$

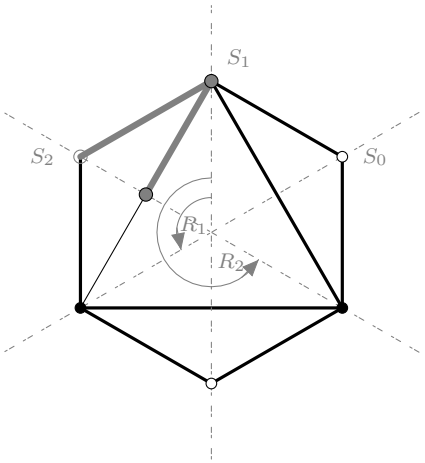
kar množica generatorjev za grupo G.

Dokaz: Naj bo $g \in G$ poljuben element in naj bo v poljubno vozlišče v fundamentalni domeni $\mathcal{F}$. Izberimo pot p, ki povezuje vozlišče v z vozliščem $g \cdot v$ in naj bo $\{\mathcal{F}, g_1\mathcal{F}, g_2\mathcal{F}, ..., g_n\mathcal{F} = g \cdot \mathcal{F}\}$ tako končno zaporedje slik fundamentalne domene, da velja:

1. celotna pot p je vsebovana v $\bigcup g_i\mathcal{F}$ in
2. $g_i\mathcal{F} \cap g_{i+1}\mathcal{F} \neq \emptyset$ za $i \in \{0, 1, ..., n-1\}$, kjer je g_0 definirana kot identiteta.

Ker je $\mathcal{F} \cap g_1\mathcal{F} \neq \emptyset$, je $g_1 \in S$ po definiciji. Podobno $g_1\mathcal{F} \cap g_2\mathcal{F} \neq \emptyset$ implicira dejstvo $\mathcal{F} \cap g_1^{-1}g_2\mathcal{F}$, torej je $g_1^{-1}g_2 \in S$ in tako je g_2 produkt elementov v S. Če nadaljujemo v tej smeri, vidimo, da mora tudi $g_n = g$ biti produkt elementov v S. Torej je S res množica generatorjev za grupo G, saj je poljuben element v grupi predstavljen kot produkt elementov v množici S. ∎

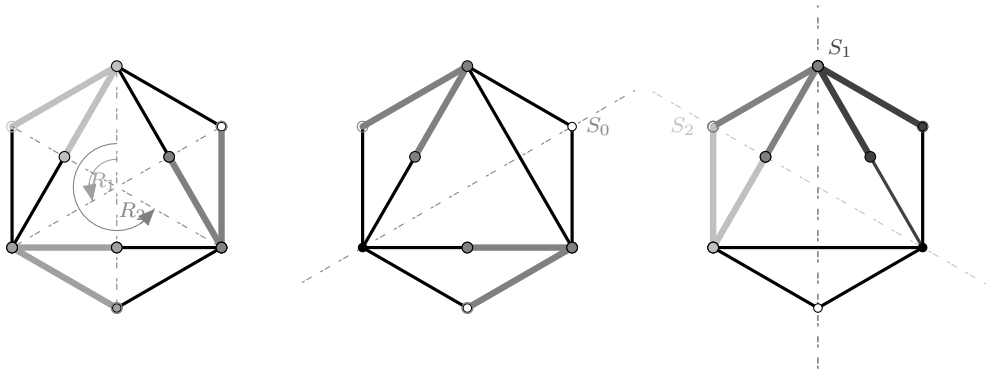
Primer 3.68. Vrnimo se k zgornjemu primeru 3.66. Naj bo torej Γ graf na sliki 30 in naj bo $\mathcal{F}$ s sivo barvo označena fundamentalna domena za delovanje grupe $\mathrm{Sym}(\Gamma) \cong D_3$. Zanima nas, kako izgleda množica generatorjev po izreku 3.67. Preverimo, kateri elementi $g \in \mathrm{Sym}(\Gamma) = \{I, R_1, R_2, S_0, S_1, S_2\}$ ustrezajo pogojem za množico generatorjev.



Slika 30: Na sliki je narisan graf Γ, na njem je s sivo barvo označena tudi njegova fundamentalna domena $\mathcal{F}$ ter elementi grupe $\mathrm{Sym}(\Gamma)$.

Preverimo torej, kateri izmed elementov v grupi $\mathrm{Sym}(\Gamma) \setminus \{I\}$ zadoščajo pogoju $g \cdot \mathcal{F} \cap \mathcal{F} \neq \emptyset$ za množico generatorjev po izreku 3.67.

Slike fundamentalne domene $\mathcal{F}$ po delovanju elementov R_1, R_2 in S_0 imajo prazen presek s fundamentalno domeno $\mathcal{F}$, kot je to razvidno iz slik 31a in 31b, medtem ko imata sliki $S_1\mathcal{F}$ in $S_2\mathcal{F}$ s fundamentalno domeno $\mathcal{F}$ neprazen presek, kar je prikazano na sliki 31c. Torej je množica generatorjev grupe $\mathrm{Sym}(\Gamma)$ sestavljena iz dveh sosednjih zrcaljenj S_1 in S_2.



(a) Sliki $\mathcal{F}$ po rotacijah R_1 in R_2. (b) Zrcaljenje $\mathcal{F}$ preko osi S_0. (c) Zrcaljenje $\mathcal{F}$ preko osi S_1 in S_2.

Slika 31: Slike fundamentalnih domen $R_1\mathcal{F}$, $R_2\mathcal{F}$, $S_0\mathcal{F}$, $S_1\mathcal{F}$ in $S_2\mathcal{F}$.

Fundamentalne domene se izkažejo za priročne pri iskanju množic generatorjev, med drugim pa so v pomoč tudi pri ugotavljanju indeksa podgrup.

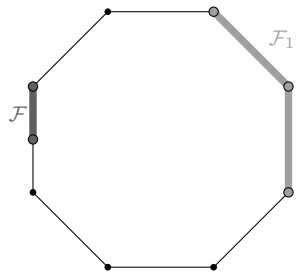
Izrek 3.69. *Naj grupa G deluje na graf Γ s fundamentalno domeno $\mathcal{F}$. Predpostavimo še, da če je $g \cdot \mathcal{F} = \mathcal{F}$, potem je $g = e \in G$. Če je H podgrupa grupe G in je fundamentalna domena za inducirano delovanje podgrupe H na graf Γ unija n kopij domene $\mathcal{F}$, kjer je $n \in \mathbb{N} \cup \{\infty\}$, potem je indeks podgrupe H v grupi G enak n.*

Dokaz: To je v osnovi posledica izreka 3.24. Ker noben element grupe G, ki je različen od identitete, ne fiksira $\mathcal{F}$, obstaja točka $x \in \mathcal{F}$, ki se giblje prosto pod delovanjem grupe G. Torej obstaja bijekcija med elementi grupe G in elementi v orbiti $\mathrm{Orb}(x)$ elementa $x \in \mathcal{F}$.

Izrazimo našo fundamentalno domeno $\mathcal{F}$ za delovanje $H \curvearrowright \Gamma$ kot eksplicitno unijo kopij domene $\mathcal{F}$: $\mathcal{F}_H = \bigcup_{i=1}^{n} g_i \cdot \mathcal{F}$, kjer so g_i različni elementi grupe G in je $n \in \mathbb{N} \cup \{\infty\}$. Ker je $\mathcal{F}_H$ fundamentalna domena za delovanje podgrupe H, velja: če je $g \in G$, potem je $g \cdot x = g_i h \cdot x$ za enega od zgornjih $g_i \in G$. Zato je $G = \bigcup_{i=1}^{n} g_i \cdot H$. Velja še več, če je $g_i \cdot H \cap g_j \cdot H \neq \emptyset$, potem je $g_i g_j^{-1} \in H$, kar pa je v nasprotju z dejstvom, da je $\mathcal{F}_H$ fundamentalna domena. Zato elementi g_i tvorijo množico odsekov za podgrupo H v grupi G in je indeks podgrupe H v grupi G enak $[G : H] = n$. ∎

Primer 3.70. Naj bo C_8 povezan graf z osmimi vozlišči, ki so povezani v en cikel. Simetrijska grupa grafa C_8 je kar diedrska grupa D_8. Za delovanje $D_8 \curvearrowright C_8$ je za fundamentalno domeno $\mathcal{F}$ dovolj vzeti eno vozlišče in polovično povezavo.

Grupa $\mathrm{Sym}(C_8)$ ima ciklično podgrupo $\mathbb{Z}_4$, ki si jo lahko predstavljamo kot rotacije za kot $\frac{\pi}{2} \cdot n$. Fundamentalna domena $\mathcal{F}_1$ za delovanje $\mathbb{Z}_4 \curvearrowright C_8$ je sestavljena iz treh vozlišč, ki so med seboj povezana z dvema povezavama. Vse to se lahko zasledimo na sliki 32.



Slika 32: Fundamentalna domena $\mathcal{F}$ za delovanje D_8 je označena na levi strani grafa C_8, fundamentalna domena $\mathcal{F}_1$ za delovanje podgrupe $\mathbb{Z}_4$ pa je označena na desni strani grafa C_8.

Opazimo lahko, da je fundamentalna domena za podgrupo $\mathbb{Z}_4$ unija štirih kopij fundamentalne domene $\mathcal{F}$ za delovanje $\mathrm{Sym}(C_8) \cong D_8$. Po izreku 3.69 je indeks ciklične podgrupe $\mathbb{Z}_4$ v diedrski grupi D_8 enak $[D_8 : \mathbb{Z}_4] = 4$.

3.8 Besede in poti

V tem poglavju bomo nanizali kar nekaj novih definicij in s to množico definicij bomo vstopili v teorijo formalnih jezikov, mi pa si bomo ogledali njen vpliv na teorijo grup. Razdelek je povzet po knjigi [10] ter članku v zborniku [3].

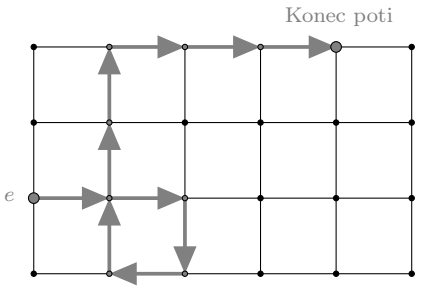
Definicija 3.71. Za dano množico S se končno zaporedje elementov iz S z možnostjo ponavljanja elementov imenuje *beseda*. Začetno množico S poimenujemo *abeceda*. Zbirko vseh besed, vključno s *prazno besedo* ϵ, ki je niz 0 elementov, označimo z oznako S^*. Z oznako S^{-1} bomo označili množico formalnih inverzov elementov iz množice S. Za lažje razumevanje si oglejmo primer: če je množica $S = \{a, b\}$, potem je $S^{-1} = \{a^{-1}, b^{-1}\}$. Sedaj lahko tvorimo množico $(S \cup S^{-1})^*$, katere elementi so končni nizi elementov iz množic S in S^{-1}. Poglejmo si primer: če je $S = \{a, b\}$, potem so b, aba^{-1}, ab in $aba^{-1}a$ različni si elementi v množici $(S \cup S^{-1})^*$.

K definicijam dodajmo dva dogovora:

- Če je $a \in S^{-1}$ tak, da je $a = x^{-1}$ za nek $x \in S$, potem lahko za alternativno oznako za x vzamemo kar a^{-1}. V bistvu rečemo, da je $(x^{-1})^{-1}$ kar x.
- Dovoljeni so tudi formalni inverzi besed, ne le posameznih elementov. Torej, če je beseda $\omega = x_1 x_2 ... x_{k-1} x_k \in (S \cup S^{-1})^*$, potem je $\omega^{-1} = x_k^{-1} x_{k-1}^{-1} ... x_2^{-1} x_1^{-1} \in (S \cup S^{-1})^*$.

Za vsako besedo $\omega \in (S \cup S^{-1})^*$ obstaja asociirana pot povezav v Cayleyjevem grafu $\Gamma_{G,S}$ za dano grupo G z množico generatorjev S. Označimo jo s p_ω. Pot se začne pri vozlišču, ki je v korespondenci z nevtralnim elementom e, nato pa prečka povezave grafa $\Gamma_{G,S}$, kot to narekujejo elementi v besedi ω.

Zgled 3.72. Na sliki 33 si oglejmo, kako izgleda beseda $\omega = xxy^{-1}x^{-1}yyyxxx$ kot pot v Cayleyjevem grafu grupe $\mathbb{Z} \times \mathbb{Z}$, ki je generirana z $x = (1, 0)$ in $y = (0, 1)$.



Slika 33: Pot povezav p_ω, ki jo opiše beseda $\omega = xxy^{-1}x^{-1}yyyxxx$.

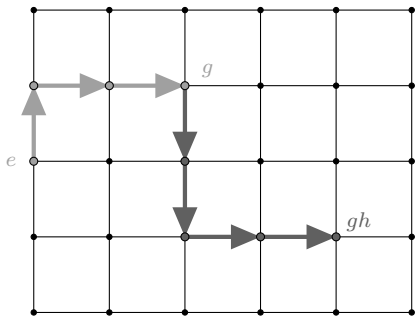
Za dano besedo ω bo pot $p_\omega : [0, 1] \to \Gamma_{G,S}$ povezala vozlišče, ki predstavlja identiteto, z vozliščem, ki je v korespondenci s tistim elementom v grupi G, ki je pridobljen z izračunom produkta elementov v besedi ω.

Zgornje velja tudi v obratno smer: vsaka končna pot povezav v Cayleyjevem grafu opiše neko besedo, ki je sestavljena iz elementov v množici generatorjev in njihovih inverzov. Preprosto preberemo oznake na povezavah, ki si sledijo in besedi dodamo inverz elementa, če potujemo v nasprotno smer, kot je povezava usmerjena.

Sledi torej, da za dano grupo G in končno množico generatorjev S obstaja bijekcija med končnimi potmi povezav v Cayleyjevem grafu $\Gamma_{G,S}$, ki se začnejo v vozlišču, ki predstavlja identiteto grupe, in med besedami v množici $(S \cup S^{-1})^*$.

Prav zaradi te povezave med besedami in potmi, lahko na Cayleyjev graf grupe G gledamo kot na neke vrste kalkulator za grupo G. Naj bosta g in h elementa grupe G, ω_g in ω_h pa naj bosta besedi v $(S \cup S^{-1})^*$, ki predstavljata elementa g in h. Za izračun produkta $g \cdot h$ lahko sledimo poti povezav p_g, opisano z besedo ω_g, in nato nadaljujemo pri vozlišču, ki predstavlja element g v Cayleyjevem grafu, odtod pa sledimo poti povezav p_h, opisano z besedo ω_h.

Zgled 3.73. Na konkretnem primeru si oglejmo, kako lahko uporabimo Cayleyjev graf kot kalkulator za grupo G. Naj bo grupa G enaka $\mathbb{Z} \times \mathbb{Z}$ in njena množica generatorjev naj bo sestavljena iz $x = (1, 0)$ in $y = (0, 1)$. Vzemimo elementa $g = yx^2$ in $h = y^{-2}x^2$. S pomočjo poti povezav v Cayleyjevem grafu izračunajmo produkt $g \cdot h$. Kot je prikazano na sliki 34 je le-ta enak $g \cdot h = yx^2y^{-2}x^2$. Iz slike je razvidno tudi, da lahko $g \cdot h$ izrazimo kot $g \cdot h = x^4y^{-1}$.



Slika 34: Izračun produkta $g \cdot h$ s pomočjo poti p_g in p_hv Cayleyjevem grafu, kjer sta $g = yx^2$ in $h = y^{-2}x^2$.

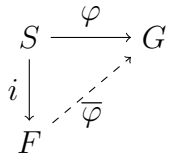
4 Proste grupe

Proste grupe imajo ključen pomen pri študiju neskončnih grup, ponudijo pa nam tudi zglede, ki prikažejo moč mešanja algebraičnih in geometrijskih pristopov. Proste grupe lahko definiramo na številne načine, v naslednjem razdelku bomo predstavili proste grupe preko njihove univerzalne lastnosti, kasneje pa bomo podali še standardno definicijo, ki je bolj formalna in algebraična. Drug pogost pristop za definicijo prostih grup je tudi uporaba delovanj grup na drevesa. To perspektivo bomo natančneje predstavili v naslednjem poglavju. Slabost formalne definicije je ta, da ne predstavi moči geometrijske predstave, je pa to pogosto najlažja in najbolj uporabna definicija, ko poskušamo pokazati, da je dana grupa prosta grupa.

4.1 Definicija in konstrukcija prostih grup

Vsak vektorski prostor vsebuje posebne množice generatorjev, med njimi so tudi tiste, katere generatorji so prosti, kot je le mogoče. To pomeni, da imajo čim manj linearnih algebraičnih relacij med njimi. Primer takšnih so linearno neodvisni generatorji. Tudi v teoriji grup lahko formuliramo pojem proste množice generatorjev. Razdelek o definiciji prostih grup temelji na knjigi [9].

Definicija 4.1. Naj bo S množica. Grupa F je *prosto generirana z množico* S, če ima F naslednjo *univerzalno lastnost*: za vsako grupo G in vsako preslikavo $\varphi\colon S \to G$ obstaja enoličen homomorfizem grup $\overline{\varphi}\colon F \to G$, ki razširja φ:



Grupa je *prosta*, če vsebuje *prosto množico generatorjev.*

Zgled 4.2. Oglejmo si nekaj primerov prosto generiranih grup:

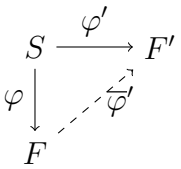
- Grupa $(\mathbb{Z}, +)$ je prosto generirana z množico $\{1\}$, ni pa prosto generirana z množico $\{2, 3\}$.
- Trivialna grupa $\{e\}$ je prosto generirana s prazno množico.

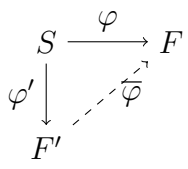
Omenjena univerzalna lastnost prostih grup nam omogoča, da dokažemo, da so objekti z univerzalno lastnostjo prostih grup v primernem smislu enolični. V naslednjem razdelku bomo pokazali, da za vsako množico obstaja grupa, ki je prosto generirana s to množico.

Trditev 4.3. *Naj bo S poljubna množica. Potem obstaja največ ena grupa, ki je prosto generirana z množico S. Ta grupa je do kanoničnega izomorfizma natančno določena.*

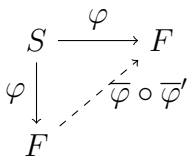
Dokaz: Zgornjo trditev bomo dokazali s protislovjem in sicer tako, da bomo domnevali, da obstajata dva objekta z omenjeno univerzalno lastnostjo: F in F' naj bosta dve grupi, ki sta prosto generirani z množico S. Vložitev S v F in F' zaporedoma označimo s φ in φ'.

Ker je F prosto generirana z množico S, nam po univerzalni lastnosti zagotavlja obstoj takega homomorfizma grup $\overline{\varphi}'\colon F \to F'$, da velja $\overline{\varphi}' \circ \varphi = \varphi'$. Analogno obstaja tudi homomorfizem grup $\overline{\varphi}\colon F' \to F$, ki zadošča $\overline{\varphi} \circ \varphi' = \varphi$. To lahko prikažemo tudi s pomočjo diagramov:





Pokažimo sedaj, da veljata enakosti $\overline{\varphi} \circ \overline{\varphi}' = id_F$ in $\overline{\varphi}' \circ \overline{\varphi} = id_{F'}$, s tem pokažemo tudi, da sta φ in φ' izomorfizma. Kompozitum $\overline{\varphi} \circ \overline{\varphi}'\colon F \to F$ je homomorfizem grup, ki tvori naslednji komutativen diagram:



Še več, tudi id_F je homomorfizem grup, ki ustreza diagramu zgoraj. Ker je F prosto generirana z množico S, nam enoličnost univerzalne lastnosti pove, da sta ta dva homomorfizma enaka: $\overline{\varphi} \circ \overline{\varphi}' = id_F$. Povsem analogno dokažemo tudi drugo enakost $\overline{\varphi}' \circ \overline{\varphi} = id_{F'}$.

Ti izomorfizmi so kanonični v smislu, da inducirajo identitetno preslikavo na S in so tudi edini izomorfizmi med F in F', ki razširijo identiteto na S. ∎

4.2 Konstrukcija prostih grup

V tem razdelku, ki je povzet po knjigi [9], si bomo ogledali, kako lahko skonstruiramo prosto grupo iz poljubne množice S. Zato si oglejmo naslednji izrek:

Izrek 4.4. *Naj bo S množica. Potem obstaja grupa, ki je prosto generirana z množico S.*

Preden izrek dokažemo, omenimo samo, da je ta grupa po prejšnji trditvi enolična do izomorfizma natančno. Zato jo lahko označimo z oznako $F(S)$.

Dokaz: Konstrukcija proste grupe sloni na ideji, da konstruiramo grupo, sestavljeno iz besed, ki nastanejo iz elementov množice S in njihovih formalnih inverzov, ki se nahajajo v množici S^{-1}. Obravnavali bomo besede, ki nastanejo iz abecede $A := (S \cup S^{-1})$, z A^* pa bomo označili množico vseh besed nad abecedo A.

Prvi korak konstrukcije je ta, da definiramo kompozitum $A^* \times A^* \to A^*$ preko stika besed. Ta binarna operacija je asociativna in prazna beseda ϵ je njen nevtralni element.

V drugem koraku konstrukcije definiramo $F(S) := A^*/\sim$. Tu je $\sim$ ekvivalenčna relacija, ki je definirana z

$$\begin{aligned} xss^{-1}y &\sim xy, \ \forall x, y \in A^*, \ \forall s \in S, \\ xs^{-1}sy &\sim xy, \ \forall x, y \in A^*, \ \forall s \in S. \end{aligned}$$

Ekvivalenčne razrede glede na ekvivalenčno relacijo $\sim$ bomo označili z $[\cdot]$. Stik besed v A^* inducira dobro definirano binarno operacijo $F(S) \times F(S) \to F(S)$ z $[x] \cdot [y] = [xy]$ za vsaki dve besedi $x, y \in A^*$. Dokažimo sedaj, da je množica $F(S)$ z binarno operacijo $\cdot$, ki je predstavljena s stikom besed, grupa:

- Asociativnost operacije $\cdot$ je podedovana iz asociativnosti operacije v A^*.
- Ekvivalenčni razred $[\epsilon]$ je nevtralni element za to operacijo.
- Obstoj inverzov bomo poskušali dokazati z indukcijo čez dolžino besed. Zato definiramo preslikavo $I\colon A^* \to A^*$ s predpisi

  $$\begin{aligned} I(\epsilon) &:= \epsilon, \\ I(sx) &:= I(x)s^{-1}, \\ I(s^{-1}x) &:= I(x)s, \end{aligned}$$

  za vse $x \in A^*$ in vse $s \in S$. Indukcija nam pokaže, da je $I(I(x)) = x$ in

  $$[I(x)] \cdot [x] = [I(x)x] = [\epsilon]$$

  za vsak $x \in A^*$. Tako smo pokazali, da v $F(S)$ obstajajo inverzi.

Torej množica $F(S)$ zadošča aksiomatičnemu opisu grup.

Preostane nam le še dokaz, da je grupa $F(S)$ prosto generirana z množico S. Naj bo $i\colon S \to F(S)$ taka preslikava, ki pošlje črko iz množice $S \subset A^*$ v njen ekvivalenčni razred v $F(S)$. Po naši konstrukciji je $F(S)$ generirana s podmnožico $i(S) \subset F(S)$. Pokažimo, da $F(S)$ zadošča univerzalni lastnosti prostih grup: za vsako grupo G in vsako preslikavo $\varphi\colon S \to G$ obstaja tak enoličen homomorfizem grup $\overline{\varphi}\colon F(S) \to G$, da velja $\overline{\varphi} \circ i = \varphi$. S pomočjo danega φ induktivno definirajmo preslikavo $\varphi^*\colon A^* \to G$ tako, da za vsak $s \in S$ in vsak $x \in A^*$ velja

$$\begin{aligned} \epsilon &\mapsto e, \\ sx &\mapsto \varphi(s) \cdot \varphi^*(x), \\ s^{-1}x &\mapsto (\varphi(s))^{-1} \cdot \varphi^*(x). \end{aligned}$$

Definicija φ^* je združljiva z ekvivalenčno relacijo $\sim$ na množici A^*, ker je združljiva z dano množico generatorjev za $\sim$. Za vse $x, y \in A^*$ pa velja še

$$\varphi^*(xy) = \varphi^*(x) \cdot \varphi^*(y).$$

Zato φ^* porodi dobro definirano preslikavo $\overline{\varphi}\colon F(S) \to G$ z $[x] \mapsto [\varphi^*(x)]$. Preko konstrukcije $\overline{\varphi} \circ i = \varphi$ vidimo, da je to homomorfizem grup. Velja še več: ker je množica $i(S)$ generirala $F(S)$, ne obstaja noben drug homomorfizem grup.

Da bi pokazali, da je grupa $F(S)$ prosto generirana z množico S, moramo dokazati še, da je preslikava i injektivna. Potem bomo lahko z i identificirali množico S s svojo sliko v $F(S)$. Za dokaz injektivnosti vzemimo različna elementa $s_1, s_2 \in S$. Ker i preslika črko v njen ekvivalenčni razred, torej $i(s_1) = [s_1]$ in $i(s_2) = [s_2]$, ta dva ekvivalenčna razreda pa sta si v osnovi različna, ker posamezna črka tvori svoj ekvivalenčni razred. Torej je preslikava i res injektivna in s tem je dokaz končan. ∎

Preko konstrukcije vidimo, da lahko proste grupe namesto z univerzalno lastnostjo definiramo še na en način, ki je mogoče bolj formalen in algebraičen. Zaradi različne narave problemov, ki nas zanimajo in ki vsebujejo proste grupe, se včasih izkaže, da je ena definicija bolj primerna kot druga.

4.3 Proste grupe in reducirane besede

Konstrukcija $F(S)$ je bila sestavljena iz množice vseh besed iz elementov v množici S in njihovih formalnih inverzov s pomočjo kvocientov na določeno ekvivalenčno relacijo. Ta konstrukcija je tehnično lepa, ima pa to slabost, da je iskanje ekvivalenčne relacije lahko precej zamudno. Zato si poglejmo še alternativno konstrukcijo prostih grup s pomočjo reduciranih besed. Ta pristop ima to prednost, da je vsak element grupe predstavljen s kanonično besedo. Razdelek je povzet po knjigah [9] in [10].

Definicija 4.5. Naj bo S množica in $(S \cup S^{-1})^*$ množica vseh besed nad množico S in množico formalnih inverzov elementov v S. Naj bo $n \in \mathbb{N}$ in $s_1, s_2, ..., s_n \in (S \cup S^{-1})$. Beseda $s_1 s_2 ... s_n$ je *reducirana beseda*, če veljata neenakosti $s_{j+1} \neq s_j^{-1}$ in $s_{j+1}^{-1} \neq s_j$ za vse $j \in \{1, 2, ..., n-1\}$. Velja tudi dogovor, da je prazna beseda ϵ reducirana. Z $F_{red}(S)$ označimo množico vseh reduciranih besed v $(S \cup S^{-1})^*$.

Trditev 4.6. *Naj bo S množica.*

1. *Množica $F_{red}(S)$ tvori grupo z binarno operacijo, ki je podana s kompozitumom*

$$F_{red}(S) \times F_{red}(S) \to F_{red}(S),$$
$$(s_1 ... s_n, s_{n+1} ... s_m) \mapsto (s_1 ... s_{n-r} s_{n+1+r} ... s_m),$$

   kjer sta $s_1 ... s_n$ in $s_{n+1} ... s_m$ elementa v množici $F_{red}(S)$ in je $r := \max\{k \in \{0, ..., \min\{n, m-1\}\} \mid s_{n-j} = s_{n+1+j}^{-1} \vee\ s_{n-j}^{-1} = s_{n+1+j}$ za vsak $j \in \{0, ..., k-1\}\}$.

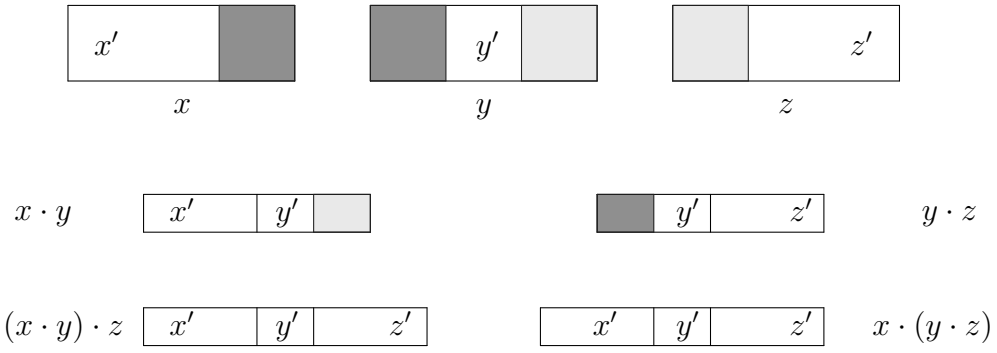
2. *Grupa $F_{red}(S)$ je prosto generirana z množico S.*

Dokaz: Najprej se lotimo dokazovanja prve točke zgornje trditve in sicer z dokazovanjem aksiomov, ki jim mora zadoščati množica $F_{red}(S)$, da jo lahko označimo za grupo.

Binarna operacija je dobro definirana, saj če sta dve besedi sestavljeni s pomočjo naše binarne operacije, potem je sestavljena beseda reducirana že po konstrukciji. Množica ima nevtralni element enak prazni besedi ϵ. Hitro tudi vidimo, da vsaka reducirana beseda dovoli inverz glede na našo operacijo. To pokažemo tako, da vzamemo poljubno reducirano besedo, jo invertiramo, kot smo vajeni invertirati besede. Vidimo, da je tudi inverz dane reducirane besede reduciran.

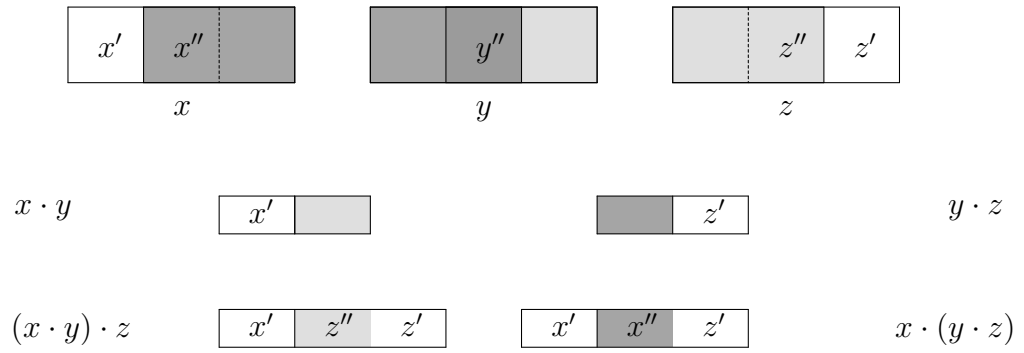
Dokazati moramo še asociativnost naše binarne operacije. Namesto formalnega dokaza z uporabo številnih indeksov, skicirajmo dokaz grafično. Naj bodo $x, y, z \in F_{red}(S)$. Želimo pokazati, da zanje velja asociativnostni zakon $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. Pri kompozitumu dveh reduciranih besed moramo po definiciji odstaniti maksimalna območja reduciranja, kjer se dve besedi srečata. Pri tem lahko ločimo dva primera:

- če se območja reduciranja besed x, y in y, z ne sekajo pri y, potem očitno velja asociativnostni zakon, kar je razvidno iz slike 36.



Slika 36: Asociativnost binarne operacije v $F_{red}(S)$ v primeru, ko se območja reduciranja ne prekrivajo.

- Če imajo območja reduciranja besed x, y in y, z netrivialen presek y'' pri y, potem asociativnostni zakon sledi iz previdnega opazovanja območij reduciranj v x in z ter v njunih sosednjih območjih, kot je to prikazano spodaj na sliki 37. Opaziti moramo, da prekrivanje v y'' povzoči, da območji x'' in z'' sovpadata, torej sta oba inverza y''.



Slika 37: Asociativnost kompozituma v $F_{red}(S)$ v primeru, ko se območja reduciranja prekrivajo.

Dokazali smo, da množica $F_{red}(S)$ skupaj z zgoraj definirano binarno operacijo zadošča aksiomom za grupo.

Preostane nam še dokaz druge točke naše trditve. Da je S prosta množica generatorjev grupe $F_{red}(S)$ pokažemo tako, da preverimo, ali je zadoščeno univerzalni lastnosti prostih grup. Naj bo H grupa in $\varphi\colon S \to H$ preslikava med množico S in grupo H. Z direktnim izračunom se izkaže, da je

$$\overline{\varphi} := \varphi^*|_{F_{red}(S)}\colon F_{red}(S) \to H,$$

homomorfizem grup, kjer je φ^* razširitev φ do množice $(S \cup S^{-1})^*$. Očitno je $\overline{\varphi}|_S$ enak φ. Ker pa je S množica generatorjev grupe $F_{red}(S)$, sledi, da je $\overline{\varphi}$ edini tak homomorfizem. Iz tega pa lahko zaključimo, da je grupa $F_{red}(S)$ prosto generirana z množico S. ∎

Kot direktno posledico dokaza druge lastnosti v zgornji trditvi dobimo naslednjo posledico:

Posledica 4.7. *Naj bo S množica. Vsak element $F(S) = (S \cup S^{-1})^*/_\sim$ lahko predstavimo z natanko eno reducirano besedo nad množico $(S \cup S^{-1})$.*

4.4 Nekaj lastnosti prostih grup

Lastnosti, ki so navedene v tem razdelku, so povzete iz knjige [9]. Za začetek raziščimo lastnost, ki pravi, da imajo vse končne proste množice generatorjev enako moč.

Trditev 4.8. *Naj bo F prosta grupa na končnih množicah S_1 in S_2. Potem je $|S_1| = |S_2|$.*

Dokaz: Po univerzalni lastnosti prostih grup vsaka preslikava $S_1 \to \mathbb{Z}_2$ porodi homomorfizem iz grupe F v ciklično grupo $\mathbb{Z}_2$ reda 2. Še več, vsak homomorfizem $F \to \mathbb{Z}_2$ lahko pridobimo na tak način, saj je vsak homomorfizem popolnoma definiran s svojimi vrednostmi na dani množici generatorjev. Zatorej imamo natanko $2^{|S_1|}$ različnih homomorfizmov, ki pošljejo grupo F v $\mathbb{Z}_2$. Iz tega sledi, da je $2^{|S_1|} = 2^{|S_2|}$ in posledično je $|S_1| = |S_2|$, če sta S_1 in S_2 končni množici.

■

Oglejmo si neposredno posledico zgornje trditve:

Posledica 4.9. *Naj bosta S_1 in S_2 množici ter $F(S_1)$ in $F(S_2)$ prosti grupi. Potem velja*

$$F(S_1) \cong F(S_2) \Rightarrow |S_1| = |S_2|.$$

Trditev 4.8 nam pove, da je moč proste množice generatorjev proste grupe F, ki jo večkrat poimenujemo kar *baza*, invarianta grupe F, ki karakterizira grupo F do izomorfizma natančno.

Definicija 4.10. Naj bo F prosta grupa na prosti množici generatorjev S. Potem imenujemo moč množice S *rang grupe* F.

Definicija 4.11. Naj bo $n \in \mathbb{N}$ in naj bo $S = \{x_1, x_2, ..., x_n\}$ množica n različnih elementov. Potem z $\mathbb{F}_n$ označimo grupo, ki je prosto generirana z množico S, in tej grupi $\mathbb{F}_n$ pravimo prosta grupa ranga n.

Opomba 4.12. Opazimo lahko, da če je $S_1 \subseteq S_2$, potem je podgrupa $\langle S_1 \rangle$ grupe $F(S_2)$, ki je generirana z množico S_1, tudi sama prosta grupa z bazo S_1. Iz tega sledi, da če sta m in n moči in je $n \leq m$, potem je $\mathbb{F}_n$ vsebovana v $\mathbb{F}_m$.

Za razliko od podprostorov vektorskih prostorov, ki ne morejo imeti večjih dimenzij kot prvoten podprostor, pa imajo proste grupe ranga 2 podgrupe, ki so izomorfne prostim grupam višjega ranga. To bomo pokazali kasneje v poglavju 4.6.

Lotimo se še raziskovanja lastnosti, da lahko končno generirane grupe karakteriziramo kot kvociente končno generiranih prostih grup.

Posledica 4.13. *Grupa je končno generirana, če in samo če je kvocient neke končno generirane proste grupe. Z drugimi besedami: grupa G je končno generirana, če in samo če obstaja končno generirana prosta grupa F in surjektiven homomorfizem grup $F \to G$.*

Dokaz: Kvocienti končno generiranih grup so končno generirani, saj je slika končne množice generatorjev končna množica generatorjev kvocienta.

Nasprotno, naj bo grupa G generirana s končno množico $S \subset G$. Naj bo F prosta grupa, ki je generirana z množico S. Potem je grupa F končno generirana. Uporabimo univerzalno lastnost proste grupe F, da najdemo homomorfizem grup $\pi\colon F \to G$, ki bo identiteta na S. Ker množica S generira grupo G in ker S leži v sliki homomorfizma π, sledi, da je $\operatorname{im} \pi = G$. ■

4.5 Cayleyjevi grafi prostih grup

Ugotovitve tega razdelka so zbrane iz knjig [9] in [10]. Izkaže se, da lahko s pomočjo dreves kombinatorično karakteriziramo proste grupe, kar nam povesta naslednja dva izreka.

Izrek 4.14. *Naj bo F prosta grupa, ki je prosto generirana z množico $S \subset F$. Pripadajoči Cayleyjev graf $\Gamma_{F,S}$ je drevo.*

Primer 4.15. Oglejmo si primere grup, ki niso proste grupe, a imajo kljub temu za Cayleyjev graf drevo:

- Cayleyjev graf grupe $\mathbb{Z}/2\mathbb{Z}$ glede na množico generatorjev $\{1\}$ je sestavljen iz dveh vozlišč, povezanih z eno povezavo. Tu smo se osredotočili na definicijo Cayleyjevih grafov, ki nam poda neusmerjen graf. Potem je ta graf očitno drevo, grupa $\mathbb{Z}/2\mathbb{Z}$ pa ni prosta.

- Cayleyjev graf aditivne grupe $\mathbb{Z}$ z množico generatorjev $\{-1, 1\}$ sovpada s Cayleyjevim grafom grupe $\mathbb{Z}$ z enim generatorjem $\{1\}$. Dobljeni Cayleyjev graf je drevo, množica $\{-1, 1\}$ pa ni prosta množica generatorjev.

Izrek 4.16. *Naj bo G grupa in $S \subset G$ množica generatorjev, ki zadošča neenakosti $s \cdot t \neq e$ za vse $s, t \in S$, kjer je e nevtralni element grupe G. Če je Cayleyjev graf $\Gamma_{G,S}$ drevo, potem je S prosta množica generatorjev grupe G.*

Morda je intuitivno jasno, da prosta množica generatorjev ne vodi do ciklov v pripadajočem Cayleyjevem grafu in obratno, a za formalni dokaz potrebujemo opis prostih grup s pomočjo reduciranih besed. Najprej se lotimo dokaza izreka 4.14, ki pravi, da je Cayleyjev graf prostih grup drevo.

Dokaz: Naj bo F prosto generirana grupa z množico S. Po trditvi 4.6, v kateri smo prikazali proste grupe s pomočjo reduciranih besed, je grupa F izomorfna grupi $F_{red}(S)$ preko izomorfizma, ki je identiteta na S. Zato lahko brez škode za splošnost domnevamo, da je F kar $F_{red}(S)$.

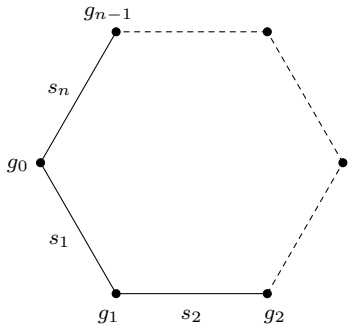
Pokažimo, da je Cayleyjev graf $\Gamma_{F,S}$ drevo. Ker množica S generira grupo F, je Cayleyjev graf $\Gamma_{F,S}$ povezan. Da je $\Gamma_{F,S}$ drevo, bomo pokazali s pomočjo protislovja. Recimo, da Cayleyjev graf $\Gamma_{F,S}$ vsebuje cikel $g_0, ..., g_{n-1}$ dolžine n, kjer je $n \geq 3$. Naj bodo elementi $g_0, ..., g_{n-1}$ različni in naj velja še

$$s_{j+1} := g_{j+1} \cdot g_j^{-1} \in S \cup S^{-1},$$

za vse $j \in \{0, ..., n-2\}$ ter

$$s_n := g_0 \cdot g_{n-1}^{-1} \in S \cup S^{-1}.$$

To je prikazano tudi na sliki 38.



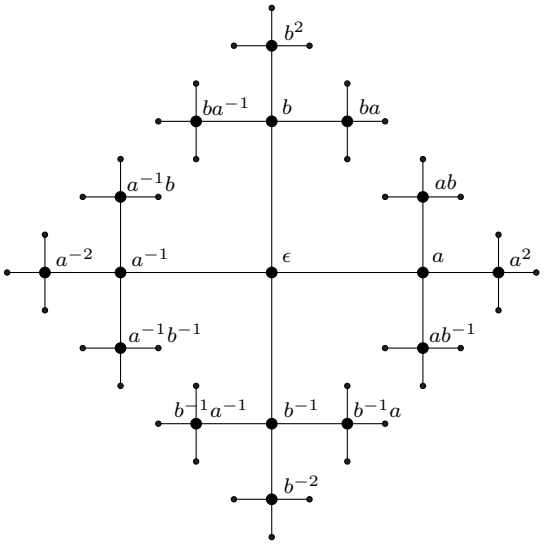
Slika 38: Cikli vodijo do reduciranih besed.

Ker so si vozlišča različna, je beseda $s_1...s_n$ reducirana. Po drugi strani pa dobimo

$$s_n...s_1 = g_0 \cdot g_{n-1}^{-1} \cdot ... \cdot g_2 g_1^{-1} g_1 g_0^{-1} = e = \epsilon$$

v grupi $F = F_{red}(S)$, kar pa je nemogoče. Prišli smo torej do protislovja z dejstvom, da se v Cayleyjevem grafu $\Gamma_{F,S}$ nahaja cikel. Ker je $\Gamma_{F,S}$ graf brez ciklov, je Cayleyjev graf grupe F s prosto množico generatorjev S drevo. ■

Primer 4.17. Oglejmo si primer Cayleyjevega grafa proste grupe $\mathbb{F}_2$ ranga 2, le-ta je prikazan na sliki 39. Naj bo S množica, ki je sestavljena iz dveh različnih si elementov $\{a, b\}$. Pripadajoč Cayleyjev graf $\Gamma_{\mathbb{F}_2,\{a,b\}}$ je regularno drevo, katerega vozlišča imajo natanko 4 sosede.



Slika 39: Del neskončnega Cayleyjevega grafa proste grupe $\mathbb{F}_2$ glede na prosto množico generatorjev $\{a, b\}$.

Za konec tega razdelka nam je preostal še dokaz izreka 4.16, ki poveže Cayleyjeve grafe, ki so drevesa, s prostimi grupami.

Dokaz: Naj bo G grupa in $S \subset G$ taka množica reduciranih generatorjev, da je pripadajoč Cayleyjev graf $\Gamma_{G,S}$ drevo. Pokazati želimo, da je S prosta množica generatorjev grupe G. Glede na trditev 4.6 je dovolj pokazati, da je grupa G izomorfna grupi $F_{red}(S)$ preko izomorfizma, ki je identičen na množici S.

Ker je $F_{red}(S)$ prosto generiran z množico S, nam univerzalna lastnost prostih grup zagotovi homomorfizem grup $\varphi\colon F_{red}(S) \to G$, ki je identiteta na S. Ker je S množica generatorjev grupe G, sledi, da je homomorfizem φ surjektiven.

Do izomorfizma med grupama $F_{red}(S)$ in G manjka še injektivnost homomorfizma φ. Pri dokazu si pomagajmo s protislovjem. Privzemimo, da homomorfizem φ ni injektiven. Naj bo $s_1...s_n \in F_{red}(S)\backslash\{e\}$, kjer so $s_1, ..., s_n \in S \cup S^{-1}$. Element $s_1...s_n$ naj bo minimalne dolžine, ki je preko homomorfizma φ preslikan v e. Ker je $\varphi|_S = id_S$ injektiven homomorfizem, velja, da je $n > 1$. Obravnavajmo naslednje primere:

- Če je $n = 2$, potem bi veljalo

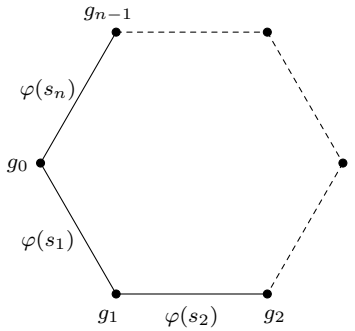
  $$e = \varphi(s_1 \cdot s_2) = \varphi(s_1) \cdot \varphi(s_2) = s_1 \cdot s_2 \in G,$$

  kar nasprotuje dejstvu, da je $s_1...s_n$ reducirana beseda in nasprotuje neenakosti $s \cdot t \neq e$ za vse $s, t \in S$.

- Če je $n \geq 3$, potem obravnavajmo niz elementov $g_0, ..., g_{n-1} \in G$, ki so dani z

  $$\begin{aligned} g_0 &:= e, \\ g_{j+1} &:= g_j \cdot \varphi(s_{j+1}), \end{aligned}$$

  za vse $j \in \{0, ..., n-2\}$.



Slika 40: Reducirane besede povzročijo obstoj ciklov.

Zaporedje $g_0, ..., g_{n-1}$ je cikel v Cayleyjevem grafu $\Gamma_{G,S}$ zaradi minimalne velikosti besede $s_1...s_n$ ter zaradi povezav $\{g_0, g_1\}, ..., \{g_{n-2}, g_{n-1}\}$ in

$$\{g_{n-1}, g_0\} = \{s_1 s_2 ... s_{n-1}, e\} = \{s_1 s_2 ... s_{n-1}, s_1 s_2 ... s_n\},$$

kjer so si elementi $g_0, ..., g_{n-1}$ med seboj različni, kar je prikazano na sliki 40. To pa je v protislovju z dejstvom, da je Cayleyjev graf $\Gamma_{G,S}$ drevo.

Iz tega lahko torej zaključimo, da mora biti homomorfizem $\varphi\colon F_{red}(S) \to G$ injektiven. Posledično sta si grupi $F_{red}(S)$ in G izomorfni. Zaključimo lahko, da je tudi G, kot je to $F_{red}(S)$, prosta grupa. ∎

4.6 Prosta grupa $\mathbb{F}_3$ je podgrupa proste grupe $\mathbb{F}_2$

Lahko je videti, da je prosta grupa ranga 2 podgrupa v prosti grupi ranga 3 ali višjega ranga: če je $\{x_1, x_2, ..., x_n\}$ baza za prosto grupo $\mathbb{F}_n$, potem nobena reducirana beseda v $\{x_1, x_2, x_1^{-1}, x_2^{-1}\}^*$ ni enaka identiteti. Zatorej je podgrupa, ki je generirana z $\{x_1, x_2\}$, prosta grupa ranga 2.

Naslednja trditev pa je presentljiva, saj kot smo omenili že v prejšnjem razdelku, lahko prosta grupa vsebuje podgrupo, ki ima višji rang kot prvotna grupa, medtem ko pri vektorskih prostorih ni mogoče, da bi vsebovali podprostor večje dimenzije kot dani prostor. Razdelek je povzet po knjigi [10].

Trditev 4.18. *Obstaja podgrupa proste grupe $\mathbb{F}_2$ s končnim indeksom, ki je prosta grupa ranga 3.*

Dokaz: Bistvenega pomena za naš dokaz je dejstvo, da lahko elementom proste grupe $\mathbb{F}_2$ pripišemo dolžine. Ker lahko vsak $g \in \mathbb{F}_2$ enolično izrazimo kot prosto reducirano besedo v množici generatorjev in njihovih formalnih inverzov, lahko definiramo dolžino elementa g kot število črk v izrazu g, ki predstavlja prosto reducirano besedo. Dolžino elementa g označimo z $|g|$. Kot primer si oglejmo naslednjo dolžino: $|x^3x^{-1}y^2xy^{-5}y| = |x^2y^2xy^{-4}| = 9$.

Ta zapis dolžine elementa grupe ima uporabno lastnost in sicer to, da velja enakost $|g| = |g^{-1}|$, saj je reduciran izraz za g^{-1} formalni inverz reduciranega izraza za g.

Naj bo H podmnožica grupe $\mathbb{F}_2$, sestavljena iz elementov sode dolžine:

$$H = \{g \in \mathbb{F}_2 \mid |g| \text{ je sodo število}\}.$$

Ker velja enakost $|g| = |g^{-1}|$, je ta množica H zaprta za inverze. Ker krajšanje podbesed v nereduciranih besedah nastopa v parih, bo veljalo, da če sta $|a|$ in $|b|$ obe sodi dolžini, bo tudi $|ab|$ sodo, čeprav je možno, da je $|ab|$ manj kot $|a| + |b|$. Torej je H zaprt za inverze in produkte, od tod pa sledi, da je H podgrupa grupe $\mathbb{F}_2$. Podgrupi H pravimo *soda podgrupa* grupe $\mathbb{F}_2$.

Ker je dolžina vsakega elementa v $\mathbb{F}_2$ bodisi soda bodisi liha, je indeks podgrupe H enak $[\mathbb{F}_2 : H] = 2$.

Dokažimo sedaj, da je soda podgrupa H proste grupe $\mathbb{F}_2$ generirana z množico $S = \{x^2, xy, xy^{-1}\}$. To bomo storili tako, da bomo pokazali, da lahko vsako reducirano besedo dolžine 2 izrazimo kot produkt elementov iz množice $S \cup S^{-1}$. Nato pa bomo nadaljevali z indukcijo.

Najprej poiščemo reducirane besede dolžine 2 iz množice $\{x, y, x^{-1}, y^{-1}\}$. Mednje spadajo besede $x^2, xy, xy^{-1}, y^2, yx, yx^{-1}, x^{-2}, x^{-1}y, x^{-1}y^{-1}, y^{-2}, y^{-1}x, y^{-1}x^{-1}$. Poskusimo sedaj izraziti te reducirane besede s pomočjo elementov v množici $S \cup S^{-1} = \{x^2, xy, xy^{-1}, x^{-2}, y^{-1}x^{-1}, yx^{-1}\}$. Nekatere izmed njih so že enake elementom v zgornji množici, zato le-teh ne bomo posebej izražali; preostale pa lahko zapišemo kot $y^2 = x^{-2} \cdot (xy)^2$, $yx = yx^{-1} \cdot x^2$, $x^{-1}y = x^{-2} \cdot xy$, $x^{-1}y^{-1} = x^{-2} \cdot xy^{-1}$, $y^{-2} = x^{-2} \cdot (xy^{-1})^2$, $y^{-1}x = y^{-1}x^{-1} \cdot x^2$.

Nadaljujmo z indukcijo. Naša indukcijska predpostavka je ta, da lahko vsako reducirano besedo sode dolžine n izrazimo kot produkt elementov iz $S \cup S^{-1}$. Vzemimo sedaj reducirano besedo ω z dolžino $|\omega| = n + 2$. Radi bi dokazali, da lahko tudi ω izrazimo kot produkt elementov iz $S \cup S^{-1}$. Zapišimo besedo ω kot

$$\omega = \omega' \cdot \omega_{n+1} \cdot \omega_{n+2},$$

kjer je ω' po indukcijski predpostavki takšna, da jo že lahko zapišemo kot produkt elementov iz $S \cup S^{-1}$. Podbeseda $\omega_{n+1} \cdot \omega_{n+2}$ v reducirani besedi ω je reducirana beseda dolžine 2, ki jo po prvem koraku indukcije tudi lahko izrazimo kot produkt elementov iz $S \cup S^{-1}$. S tem je indukcija končana. Od tod sledi, da je soda podgrupa H proste grupe $\mathbb{F}_2$ res generirana z množico $S = \{x^2, xy, xy^{-1}\}$.

Naj bodo $a = x^2$, $b = xy$, c $= xy^{-1}$ in naj bo $\omega = \omega_1\omega_2...\omega_n$ reducirana beseda v množici generatorjev $\{a, b, c\}$ in množici njihovih formalnih inverzov. Da bi dokazali, da je soda podgrupa H prosta z bazo $\{a, b, c\}$, moramo pokazati, da $\omega \neq e \in \mathbb{F}_2$.

Če zapišemo $\omega = \omega_1\omega_2...\omega_n$ s pomočjo prvotnih generatorjev, lahko v besedi pride do krajšanja elementov. Kot primer si oglejmo, ko ω vsebuje podbesedo $a^{-1}b$. Če to izrazimo s pomočjo prvotnih generatorjev, dobimo $a^{-1}b = x^{-1}x^{-1}xy = x^{-1}y$. Podobno se zgodi tudi v primeru $c^{-1}ac^{-1}b = (yx^{-1})(xx)(yx^{-1})(xy) = yxy^2$. Opazimo lahko, da je krajšanje prisotno v podbesedah oblike $c^{-1}a$ in $b^{-1}a$, le-tega pa ni v primeru podbesede oblike ac^{-1}, ko zapišemo te besede s pomočjo prvotnih generatorjev. Pretvorba besede ω iz reducirane oblike v množici $\{a, b, c, a^{-1}, b^{-1}, c^{-1}\}^*$ v besedo v množici $\{x, y, x^{-1}, y^{-1}\}^*$ se stori z zamenjavo vsakega ω_i z $\alpha_i\beta_i$, kjer sta $\alpha_i, \beta_i \in \{x, y, x^{-1}, y^{-1}\}$. Pokažimo, da če je $\beta_i = \alpha_{i+1}^{-1}$, potem je:

- $\alpha_i \neq \beta_{i+1}^{-1}$,
- $\beta_{i+1} \neq \alpha_{i+2}^{-1}$ in
- $\beta_{i-1} \neq \alpha_i^{-1}$.

Zapišimo besedo ω kot

$$\omega = \omega_1 ... \omega_{i-1}\omega_i\omega_{i+1} ... \omega_n = (\alpha_1\beta_1)...(\alpha_{i-1}\beta_{i-1})(\alpha_i\beta_i)(\alpha_{i+1}\beta_{i+1})...(\alpha_n\beta_n).$$

Oglejmo si podbesedo $\omega_{i-1}\omega_i\omega_{i+1} = (\alpha_{i-1}\beta_{i-1})(\alpha_i\beta_i)(\alpha_{i+1}\beta_{i+1})$. Naj bo $\beta_i = \alpha_{i+1}^{-1}$, to pomeni, da je konec ω_i enak začetku ω_{i+1}, ko jih zapišemo z α_j, β_j. To se lahko zgodi v primerih, ko je podbeseda $\omega_i\omega_{i+1}$ enaka aa^{-1}, bb^{-1}, cc^{-1}, $a^{-1}a$, $a^{-1}b$, $a^{-1}c$, $b^{-1}a$, $b^{-1}b$, $b^{-1}c$, $c^{-1}a$, $c^{-1}b$ ter $c^{-1}c$. Pare aa^{-1}, bb^{-1}, cc^{-1}, $a^{-1}a$, $b^{-1}b$, $c^{-1}c$ izločimo zaradi dejstva, da je ω reducirana beseda.

Oglejmo si primer, ko je podbeseda $\omega_i\omega_{i+1} = a^{-1}b$. Pobližje si oglejmo podbesedo $\omega_{i-1}a^{-1}b\omega_{i+2} = (\alpha_{i-1}\beta_{i-1})(x^{-1}x^{-1})(xy)(\alpha_{i+2}\beta_{i+2})$. Vidimo, da velja neenakost $\alpha_i \neq \beta_{i+1}^{-1}$, kar je eden od zgornjih pogojev. Ker je ω reducirana beseda, ω_{i-1} ne sme biti enaka elementu a, torej β_{i-1} ni enaka x, saj se nobeden od preostalih elementov $a^{-1}, b, b^{-1}, c, c^{-1}$ ne konča z x. S tem pa zadostimo pogoju $\beta_{i-1} \neq \alpha_i^{-1}$. Zaradi reduciranosti besede ω, tudi ω_{i+2} ne sme biti enaka b^{-1} in ker se elementi a, a^{-1}, b, c, c^{-1} ne začnejo z y^{-1}, α_{i+2}^{-1} ni enak β_{i+1}. Pokazali smo, da veljajo vse tri zgornje neenakosti.

Analogno obravnavamo še preostale primere in res se izkaže, da vsak posamezni primer zadošča zgornjim trem pogojem za α_j in $\beta_j \in \{x, y, x^{-1}, y^{-1}\}$.

Sedaj imamo vsa potrebna dejstva za dokaz, da je soda podgrupa H res prosta grupa z bazo $\{a, b, c\}$. Najprej preoblikujemo dano reducirano besedo $\omega \in \{a, b, c, a^{-1}, b^{-1}, c^{-1}\}^*$ v besedo $\alpha_1\beta_1...\alpha_n\beta_n \in \{x, y, x^{-1}, y^{-1}\}$. Od zgoraj utemeljenega vemo, da ko to preoblikovano besedo reduciramo, je največ ena izmed črk, α_i ali β_i, pokrajšana iz vsakega para. Zato je

$$|\alpha_1\beta_1 \cdot \alpha_2\beta_2 \cdot ... \cdot \alpha_n\beta_n| \geq n.$$

Iz tega sledi, da $\omega \neq e \in \mathbb{F}_2$. Torej je H res prosta grupa z bazo $\{a, b, c\}$, katere rang je enak 3. Zato lahko H označimo z $\mathbb{F}_3$. Dokazali smo presentljivo dejstvo, da se znotraj grupe $\mathbb{F}_2$ ranga 2 nahaja prosta grupa višjega ranga. ∎

4.7 Homomorfizmi prostih grup

V tem razdelku bomo opisali, kako lahko za dano grupo G definiramo homomorfizem grup $\mathbb{F}_n \to G$ preprosto z izbiro elementov za bazo $\mathbb{F}_n$. Snov v razdelku je povzeta po knjigi [10].

Izrek 4.19. *Naj bo G poljubna grupa in naj množica $\{g_1, g_2, ..., g_n\}$ predstavlja seznam elementov grupe G, kateri niso nujno različni med seboj ali netrivialni. Naj bo množica $S = \{x_1, x_2, ..., x_n\}$ baza za prosto grupo $\mathbb{F}_n$. Potem obstaja homomorfizem grup $\phi\colon \mathbb{F}_n \to G$, za katerega je $\phi(x_i) = g_i$.*

Dokaz: Iz opisa pogojev izreka vemo, kam ϕ preslika bazo $\{x_1, x_2, ..., x_n\}$ in če želimo, da je ϕ homomorfizem, mora veljati še, da je $\phi(x_i^{-1}) = g_i^{-1}$. Če je ω poljuben element proste grupe $\mathbb{F}_n$, potem lahko ω izrazimo kot $\omega = \omega_1\omega_2...\omega_k$, kjer je $\omega_i \in S \cup S^{-1}$. Definirajmo $\phi(\omega)$ kot $\phi(\omega) = \phi(\omega_1)\phi(\omega_2)...\phi(\omega_k)$.

Elementi proste grupe $\mathbb{F}_n$ so ekvivalenčni razredi besed, kjer je ekvivalenčna relacija generirana z

$$\omega_1...\omega_i x x^{-1}\omega_{i+1}...\omega_k \sim \omega_1...\omega_i\omega_{i+1}...\omega_k,$$

kjer je $x \in S \cup S^{-1}$.

Ker je naša definicija homomorfizma ϕ uporabila točno določeno besedo za predstavitev ω, moramo preveriti, da bi bil rezultat enak, če bi uporabili drugo besedo, ki bi prav tako predstavljala ω. Velja namreč

$$\begin{aligned}\phi(\omega) &= \phi(\omega_1\omega_2...\omega_k)\\ &= \phi(\omega_1)\phi(\omega_2)...\phi(\omega_k)\\ &= \phi(\omega_1)\phi(\omega_2)...\phi(\omega_i)\phi(x)\phi(x)^{-1}\phi(\omega_{i+1})...\phi(\omega_k)\\ &= \phi(\omega_1...\omega_i x x^{-1}\omega_{i+1}...\omega_k).\end{aligned}$$

Zatorej element $\phi(\omega) \in G$ ni odvisen od oblike besede, ki predstavlja besedo ω. Iz definicije tudi takoj sledi, da je $\phi(\omega^{-1}) = (\phi(\omega))^{-1}$ in da velja $\phi(\omega \cdot \omega') = \phi(\omega)\phi(\omega')$. Torej je ϕ res homomorfizem grup. ∎

Tehnika za konstrukcijo homomorfizmov, ki je bila predstavljena v dokazu zgornjega izreka, ne deluje v splošnem. Oglejmo si primer neskončne diedrske grupe $D_\infty := \langle s, t \mid s^2 = t^2 = e\rangle$, ki jo generirata dve zrcaljenji s in t. Ne obstaja homomorfizem $\phi\colon D_\infty \to \mathbb{Z}$, za katerega bi veljalo $\phi(s) = \phi(t) = 1 \in \mathbb{Z}$. Če bi tak homomorfizem obstajal, bi veljalo $\phi(s^2) = 2$, ker pa je $s^2 = e \in D_\infty$, ϕ ne bi slikal nevtralnega elementa grupe D_∞ v nevtralni element aditivne grupe $\mathbb{Z}$.

Dejstvo, da zgornja tehnika za konstrukcijo homomorfizmov deluje v primeru prostih grup, ima mnoge pomembne posledice. Ena izmed njih se glasi:

Posledica 4.20. *Vsaki dve prosti grupi ranga n sta si izomorfni.*

Dokaz: Naj bo G prosta grupa z bazo $\{x_1, x_2, ..., x_n\}$ in H prosta grupa z bazo $\{z_1, ..., z_n\}$. Po izreku 4.19 obstajata homomorfizma $\phi\colon G \to H$, za katerega velja $\phi(x_i) = z_i$ in $\psi\colon H \to G$, za katerega je $\psi(z_i) = x_i$. Iz tega sledi, da je $\psi \circ \phi$ identitetni avtomorfizem grupe G in $\phi \circ \psi$ identitetni avtomorfizem grupe H. Torej morata biti ψ in ϕ bijektivni preslikavi, od koder sledi, da sta si grupi G in H izomorfni. ∎

5 Delovanja prostih grup

V magistrskem delu smo že storili prvi korak od grup do geometrije preko Cayleyjevih grafov. Ogledali smo si še en geometrični aspekt grup preko delovanja grup, kjer smo se osredotočili na dejstvo, da lahko preko delovanja grupe na matematični objekt ustvarimo neko posplošitev grupe na simetrijsko grupo danega objekta.

V tem poglavju si bomo ogledali, kako lahko proste grupe karakteriziramo kot grupe, ki imajo za Cayleyjev graf drevo. Le-to bomo zapisali kot geometrijsko karakterizacijo prostih grup, ki pravi, da je grupa G je prosta natanko tedaj, ko omogoča prosto delovanje na drevo. Pomemben izid te karakterizacije je tudi ta, da nas vodi do elegantnega dokaza dejstva, da so podgrupe prostih grup proste.

Ogledali si bomo tudi Ping-pong lemo, ki je uporabno orodje za prepoznavanje, ali so dane grupe proste, za še posebej uporabno pa se izkaže pri dokazovanju, da so določene grupe matrik proste.

Celotno poglavje sestoji iz ugotovitev, ki se nahajajo v knjigah [9] in [10].

5.1 Prosta delovanja

Povezava med grupami in geometrijskimi objekti, na katere ta grupa deluje, je še posebej močna, če je delovanje dane grupe prosto. Bistveni zgledi prostih delovanj so naravna delovanja grup na svoje Cayleyjeve grafe, kjer je pomemben pogoj, da grupa ne vsebuje elementa reda 2.

Definicija 5.1. Naj bo G grupa in X množica. Naj bo $G \times X \to X$ delovanje G na X. To delovanje je *prosto*, če velja $g \cdot x \neq x$ za vse $g \in G \setminus \{e\}$ in vse $x \in X$. Z drugimi besedami: delovanje grupe je prosto, če in samo če vsak netrivialen element grupe deluje na X brez negibnih točk.

Primer 5.2. Nanizajmo nekaj primerov prostih delovanj:

- Oglejmo si levo translacijo kot delovanje grupe. Če je G grupa, potem je levi premik kot delovanje

$$\begin{aligned} G &\to \mathrm{Aut}(G), \\ g &\mapsto (h \mapsto g \cdot h), \end{aligned}$$

  prosto delovanje grupe G samo nase z bijekcijami.

- Naj bo $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ enotska krožnica v $\mathbb{C}$ in naj bo $\alpha \in \mathbb{R}$. Potem je rotacija

$$\begin{aligned} \mathbb{Z} \times S^1 &\to S^1, \\ (n, z) &\mapsto e^{2\pi i \cdot \alpha \cdot n} \cdot z, \end{aligned}$$

  delovanje $\mathbb{Z}$ na S^1, ki je prosto natanko tedaj, ko je α iracionalno število.

- Delovanja grupe izometrij na nek geometrijski objekt v splošnem niso nujno prosta. Grupa izomorfizmov kvadrata ne deluje prosto na kvadrat, saj so oglišča kvadrata fiksirana z zrcaljenji skozi diagonalo.

Definicija 5.3. Naj bo G grupa, ki deluje na graf Γ z množico vozlišč V in množico povezav E preko izomorfizma $\varphi\colon G \to \mathrm{Aut}(V, E)$. Delovanje φ je prosto, če za vse elemente $g \in G \setminus \{\mathrm{id}\}$, kjer je id nevtralni element grupe G, veljata naslednji neenakosti:

$$(\varphi(g))(v) \neq v \text{ za vsako vozlišče } v \in V \text{ in}$$
$$(\varphi(g))(e) \neq e \text{ za vsako povezavo } e \in E.$$

Z drugimi besedami: delovanje φ je prosto, če nobeno vozlišče in nobena povezava grafa ni fiksirana z netrivialnim elementom grupe.

Zgled 5.4. Naj bo G grupa in S množica generatorjev grupe G. Grupa G deluje na svoj Cayleyjev graf $\Gamma_{G,S}$ preko leve translacije:

$$G \to \mathrm{Aut}(\Gamma_{G,S}),$$
$$g \mapsto (h \mapsto g \cdot h).$$

Ta preslikava je dobro definirana in je homomorfizem grup.

Trditev 5.5. *Naj bo G grupa in S množica generatorjev za grupo G. Delovanje leve translacije na Cayleyjev graf $\Gamma_{G,S}$ je prosto, če in samo če množica S ne vsebuje elementa reda 2.*

Spomnimo se, da je red elementa $g \in G$ infinimum vseh $n \in \mathbb{N}$, kjer je $g^n = e$. Naš dogovor je, da je $\inf \emptyset = \infty$.

Dokaz: Delovanje na vozlišča Cayleyjevega grafa je le leva translacija grupe G samo nase, ki je prosto delovanje. Zadošča torej premisliti, pod katerimi pogoji je delovanje grupe G na povezave prosto.

Dokažimo, da če delovanje grupe G na povezave Cayleyjevega grafa $\Gamma_{G,S}$ ni prosto, potem množica S vsebuje element reda 2. Naj bo $g \in G$ in $\{v, v'\}$ povezava Cayleyjevega grafa $\Gamma_{G,S}$, za katero velja

$$\{v, v'\} = g \cdot \{v, v'\} = \{g \cdot v, g \cdot v'\}.$$

Po definiciji Cayleyjevega grafa lahko pišemo $v' = v \cdot s$ za $s \in (S \cup S^{-1}) \setminus \{e\}$. Potemtakem nastopi eden od spodnjih primerov:

- Imamo enakosti $g \cdot v = v$ in $g \cdot v' = v'$. Ker je delovanje G na vozlišča prosto, sledi, da je $g = e$.

- Imamo $g \cdot v = v'$ in $g \cdot v' = v$. Potem v G velja

$$v = g \cdot v' = g \cdot (v \cdot s) = v' \cdot s = (v \cdot s) \cdot s = v \cdot s^2,$$

od koder sledi, da je $s^2 = e$. Ker $s \neq e$, S vsebuje element reda 2.

Dokažimo trditev še v obratno smer: če je $s \in S$ reda 2, potem s fiksira povezavo Cayleyjevega grafa $\Gamma_{G,S}$ $\{e, s\} = \{s^2, s\}$. Torej delovanje leve translacije v primeru, da S vsebuje element reda 2, ni prosto. S tem je naša trditev dokazana. ∎

5.2 Ping-pong lema

Za naslednji kriterij, ki z ustreznimi delovanji pokaže, ali je dana grupa prosta, se lahko zahvalimo matematiku Felixu Kleinu.

Izrek 5.6 (Ping-pong lema)**.** *Naj bo G grupa, generirana z dvema elementoma a in b, ki imata neskončen red. Naj obstaja tako delovanje grupe G na množico X, da obstajata taki neprazni podmnožici $A, B \subset X$, za kateri velja, da B ni vsebovan v A in da za vse $n \in \mathbb{Z} \setminus \{0\}$ veljata*

$$a^n \cdot B \subset A \qquad in \qquad b^n \cdot A \subset B.$$

Potem je G prosto generirana z množico $\{a, b\}$.

Dokaz: Za dokaz Ping-pong leme moramo poiskati izomorfizem med prosto grupo $F_{red}(\{a, b\})$, ki je generirana z $\{a, b\}$, in grupo G, ki je opisana v lemi. Ta izomorfizem mora razširiti identiteto na $\{a, b\}$. Po univerzalni lastnosti prostih grup $F_{red}(\{a, b\})$ obstaja homomorfizem $\varphi\colon F_{red}(\{a, b\}) \to G$, ki razširi identiteto na $\{a, b\}$. Ker je G generiran z množico $\{a, b\}$, je ta homomorfizem φ surjektiven.

Preostane nam še, da pokažemo injektivnost homomorfizma φ. Tega se lotimo s protislovjem. Recimo, da φ ni injektiven, torej obstaja reducirana beseda $\omega \in F_{red}(\{a, b\}) \setminus \{e\}$, za katero je $\varphi(\omega) = e$. Glede na prvo in zadnjo črko v ω ločimo štiri primere:

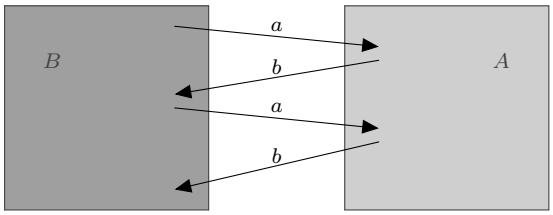
1. Beseda ω se začne in konča z netrivialno potenco a, torej lahko pišemo

$$\omega = a^{n_0} b^{m1} a^{n_1} ... b^{m_k} a^{n_k}$$

za nek $k \in \mathbb{N}$ in določene $n_0, ..., n_k, m_1, ..., m_k \in \mathbb{Z} \setminus \{0\}$. Potem je

$$\begin{aligned} B &= e \cdot B = \varphi(\omega) \cdot B \\ &= a^{n_0} b^{m1} a^{n_1} ... b^{m_k} a^{n_k} \cdot B \\ &\subset a^{n_0} b^{m1} a^{n_1} ... b^{m_k} \cdot A \\ &\subset a^{n_0} b^{m1} a^{n_1} ... a^{n_{k-1}} \cdot B \\ &\subset ... \\ &\subset a^{n_0} \cdot B \\ &\subset A, \end{aligned}$$

kar pa nasprotuje dejstvu, da B ni vsebovan v A. Preko pokazanega zgoraj si lahko zamislimo, zakaj se tej lemi reče Ping-pong lema, kar je grafično prikazano na sliki 41.



Slika 41: Shematski prikaz Ping-pong leme.

2. Beseda ω se začne in konča z netrivialno potenco elementa b. Potem je beseda $a\omega a^{-1}$ reducirana beseda, ki se začne in konča z netrivialno potenco elementa a. Ker velja $e = \varphi(a) \cdot e \cdot \varphi(a)^{-1} = \varphi(a) \cdot \varphi(\omega) \cdot \varphi(a^{-1}) = \varphi(a\omega a^{-1})$, lahko v tem primeru postopamo enako, kot smo v primeru 1.

3. Beseda ω se začne z netrivialno potenco elementa a in se konča z netrivialno potenco elementa b. Recimo, da je $\omega = a^n\omega' b^m$, kjer sta $n, m \in \mathbb{Z} \setminus \{0\}$ in ω' reducirana beseda, ki se ne začne z netrivialno potenco elementa a in ne konča z netrivialno potenco elementa b. Naj bo $r \in \mathbb{Z} \setminus \{0, -n\}$. Potem se $a^r\omega a^{-r} = a^{r+n}\omega' b^m a^{-r}$ začne in konča z netrivialno potenco elementa a in velja, da je $e = \varphi(a^r\omega a^{-r})$. Naš primer smo prevedli na pogoje prvega primera in nadaljujemo analogno kot v prvem primeru.

4. Beseda ω se začne z netrivialno potenco elementa b in konča z netrivialno potenco elementa a. Potem inverz ω spada v tretji primer in nadaljujemo enako, kot smo v postopali v tretjem primeru.

Posledično je φ injektiven in je torej $\varphi\colon F_{red}(\{a, b\}) \to G$ izomorfizem, ki razširja identiteto na $\{a, b\}$. ∎

Z uporabo Ping-pong leme lahko pokažemo, da so določene grupe matrik proste.

Zgled 5.7. Obravnavajmo matriki $a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ in $b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, kjer sta a, b elementa specialne linearne grupe $SL(2, \mathbb{Z})$. S pomočjo Ping-pong leme dokažimo, da je podgrupa grupe $SL(2, \mathbb{Z})$, generirana z $\{a, b\}$, prosta grupa ranga 2.

Grupa matrik $SL(2, \mathbb{Z})$ deluje na $\mathbb{R}^2$ z množenjem matrik. Oglejmo si podmnožici $A := \{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid |x| > |y|\}$ in $B := \{\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid |x| < |y|\}$. Množici A in B

sta neprazni in B ni vsebovana v A. Velja še več, za $n \in \mathbb{Z} \setminus \{0\}$ in vse $(x, y) \in B$ imamo

$$a^n \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 2 \cdot n \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2 \cdot n \cdot y \\ y \end{pmatrix}.$$

Velja še

$$|x + 2 \cdot n \cdot y| \geq |2 \cdot n \cdot y| - |x| \geq 2 \cdot |y| - |x| > 2 \cdot |y| - |y| = |y|,$$

torej je $a^n \cdot B \subset A$.

Na podoben način lahko pridemo do dejstva, da je $b^n \cdot A \subset B$ za vse $n \in \mathbb{Z} \setminus \{0\}$. Sedaj lahko uporabimo Ping-pong lemo in sklepamo, da je podgrupa grupe $SL(2, \mathbb{Z})$, generirana z matrikama a in b, prosto generirana z množico $\{a, b\}$.

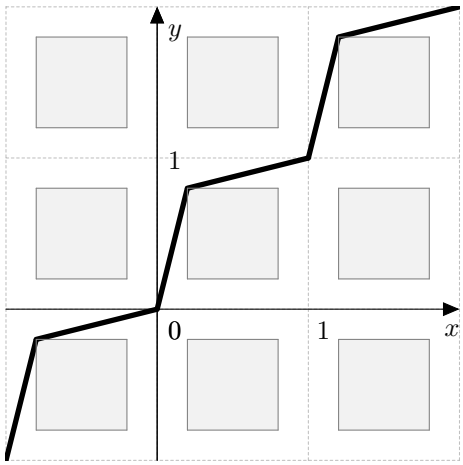
Če bi zgornji primer reševali z računanjem matrik, bi bilo to zelo zamudno in nerodno. S pomočjo ping-pong leme pa smo primer končali precej hitro in elegantno.

Zgled 5.8. Proste grupe se večkrat pojavijo kot podgrupe pomembnih razredov grup. Za zgled si oglejmo zvezno, bijektivno preslikavo $\phi \colon \mathbb{R} \to \mathbb{R}$, katere inverz je tudi zvezen. Takšni preslikavi rečemo homeomorfizem $\mathbb{R}$. Zbirka vseh takšnih zveznih preslikav tvori zelo veliko grupo, Homeo($\mathbb{R}$), katere binarna operacija je kompozitum funkcij. Nevtralni element te grupe je identična funkcija $f(x) = x$, inverzi pa obstajajo, ker smo se že pri definiciji omejili na funkcije, ki imajo inverze.

Skonstruirajmo sedaj prosto podgrupo grupe Homeo($\mathbb{R}$) z uporabo dveh eksplicitnih funkcij. Naj bo f funkcija, definirana na $[0, 1]$ z

$$\overline{f}(x) = \begin{cases} 4x, & \text{za } \ 0 \leq x \leq \frac{1}{5}, \\ \frac{4}{5} + \frac{1}{4}(x - \frac{1}{5}), & \text{za } \ \frac{1}{5} \leq x \leq 1, \end{cases}$$

ki je razširjena na realno os s predpisom $f(x) = \lfloor x \rfloor + \overline{f}(x - \lfloor x \rfloor)$. Narišimo še njen graf. Le-ta je prikazan na sliki 42.



Slika 42: Graf funkcije f, ki pošlje točke v odprtih intervalih $(i + \frac{1}{5}, i + \frac{4}{5})$ v točke v odprtih intervalih $(i + \frac{4}{5}, i + 1)$ za $i \in \mathbb{Z}$.

Definirajmo X_f kot majhne zaprte intervale okrog celih števil i,

$$X_f = \bigcup_{i\in\mathbb{Z}} [i - \frac{1}{5}, i + \frac{1}{5}].$$

Ta podmnožica realnih števil je označena na grafu funkcije f na x in y osi. Iz slike 42 lahko razberemo, da f pošlje interval $(\frac{1}{5}, \frac{4}{5})$ v interval $(\frac{4}{5}, 1)$. V splošnem pa velja

$$f[(i + \frac{1}{5}, i + \frac{4}{5})] \subset (i + \frac{4}{5}, i + 1) \subset X_f$$

za vse $i \in \mathbb{Z}$. Torej f pošlje točke, ki so izven X_f, v X_f.

Zgornji argument nam poda osnovo za argument indukcije, ki vzpostavi dejstvo, da za vsako pozitivno celo število n velja: če $x \notin X_f$, potem je $f^n(x) \in X_f$. Pomembno dejstvo je tudi to, da če $x \notin X_f$, potem je $f(x) \in (i - \frac{1}{5}, i)$ za nek $i \in \mathbb{Z}$. Ker pa je $f[(i - \frac{1}{5}, i)] \subset (i - \frac{1}{5}, i)$, je tudi $f^2(x)$ znotraj $(i - \frac{1}{5}, i)$. Za indukcijski korak lahko vzamemo, da če $x \notin X_f$, potem je $f^{n-1}(x) \in (i - \frac{1}{5}, i)$ za nek $i \in \mathbb{Z}$. Potem še zapišemo, da mora tudi $f^n(x) = f(f^{n-1}(x))$ biti v $(i - \frac{1}{5}, i) \subset X_f$.

Graf inverza funkcije f dobimo z zrcaljenjem grafa funkcije f čez premico $y = x$. Torej je graf f^{-1} tudi vsebovan v mreži, ki jo tvori X_f po x in y osi. V tem primeru velja, da če je $x \in (i-\frac{4}{5}, i-\frac{1}{5})$, je potem $f^{-1}(x) \in (i-1, i-\frac{4}{5})$, torej je $f^{-1}(x) \in X_f$. Ker pa f^{-1} pošlje interval $(i - 1, i - \frac{4}{5})$ v interval $(i - 1, i - \frac{4}{5})$, je $f^{-n}(x) \in X_f$ za vsako število $n \in \mathbb{N}$ in za $x \notin X_f$.

Naša druga funkcija je le premaknjena kopija grafa funkcije f. Definirajmo funkcijo g kot $f(x - \frac{1}{2}) + \frac{1}{2}$ in naj bo

$$X_g = \bigcup_{i\in\mathbb{Z}} [i + \frac{1}{2} - \frac{1}{5}, i + \frac{1}{2} + \frac{1}{5}].$$

Enaki argumenti kot v primeru funkcije f pokažejo, da za vsako neničelno celo število n velja, da je $g^n(x) \in X_g$, če $x \notin X_g$.

Sedaj lahko s pomočjo Ping-pong leme podpremo trditev, da je podgrupa grupe Homeo($\mathbb{R}$), ki je generirana z zgornjima funkcijama f in g, prosta grupa.

Naj bo $\omega = \omega_1\omega_2...\omega_n$ prosto reducirana beseda v $\{f, g, f^{-1}, g^{-1}\}^*$. Pokažimo, da velja $\omega \neq e$ tako, da dokažemo dejstvo, da ω ne deluje trivialno na $\mathbb{R}$. Besedo ω lahko izrazimo kot $\omega_1^{n_1}\omega_2^{n_2}...\omega_k^{n_k}$, kjer $\omega_i \neq \omega_{i+1}$ ali $\omega_i \neq \omega_{i+1}^{-1}$.

Opazimo lahko, da je $X_f \cap X_g = \emptyset$ in da $\frac{1}{4} \notin X_f \cup X_g$. Definirajmo

$$X_i = \begin{cases} X_f, & \text{če} \quad \omega_i \in \{f, f^{-1}\}, \\ X_g, & \text{če} \quad \omega_i \in \{g, g^{-1}\}. \end{cases}$$

Če na točki $x = \frac{1}{4}$ uporabimo besedo ω, dobimo

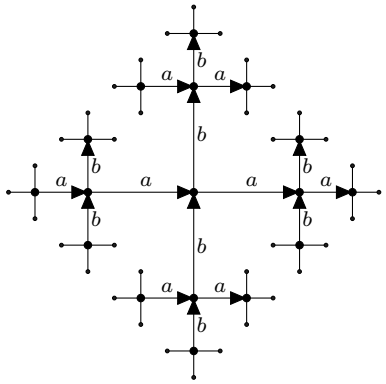
$$\begin{aligned}\omega(\frac{1}{4}) &= \omega_1^{n_1}\omega_2^{n_2}...\omega_k^{n_k}(\frac{1}{4}) \\ &\subset \omega_1^{n_1}\omega_2^{n_2}...\omega_{k-1}^{n_{k-1}}(X_k) \\ &\subset \omega_1^{n_1}\omega_2^{n_2}...\omega_{k-2}^{n_{k-2}}(X_{k-1}) \\ &\subset ... \\ &\subset \omega_1^{n_1}(X_2) \\ &\subset X_1 \subset X_f \cup X_g.\end{aligned}$$

Ampak $\frac{1}{4} \notin X_f \cup X_g$, torej velja $\omega(\frac{1}{4}) \neq \frac{1}{4}$ in posledično $\omega \neq e$. S pomočjo Ping-pong leme smo dokazali, da je podgrupa grupe Homeo($\mathbb{R}$), ki je generirana s funkcijama f in g, prosta grupa ranga 2.

Opomba 5.9. Funkciji, ki ju uporabimo v zgornjem zgledu, sta nekoliko zapleteni. V bistvu obstajajo tudi elementarne funkcije znotraj Homeo($\mathbb{R}$), ki generirajo proste podgrupe. Takšni sta na primer funkciji $f(x) = x^p$, kjer je p liho praštevilo, in $g(x) = x + 1$, ki skupaj generirata prosto podgrupo grupe Homeo($\mathbb{R}$). Vendar pa je ta navidezno dosegljiv rezultat izredno težko dokazati. Več o tem si lahko preberete v članku [13].

5.3 Prosta grupa $\mathbb{F}_2$ kot grupa drevesnih simetrij

V tem razdelku se bo počasi pokazalo, da obstaja povezava med prostimi grupami in prostim delovanjem na drevesa. En način, kako ustvariti prosto delovanje dane grupe G na graf, je preko nadgrajenega Cayleyjevega osnovnega izreka, kar tudi uporabimo v naslednji trditvi. Spomnimo se, da je Cayleyjev digraf grupe $\mathbb{F}_2$ glede na množico generatorjev $\{a, b\}$, usmerjena različica regularnega drevesa $\mathcal{T}_4$, katerega vozlišča imajo natanko 4 sosede. Ta digraf je prikazan na sliki 43.



Slika 43: Usmerjeno regularno 4-valentno drevo $\mathcal{T}_4$, ki je Cayleyjev digraf proste grupe $\mathbb{F}_2$ glede na množico generatorjev $\{a, b\}$.

Ker vsaka grupa deluje na svoj Cayleyjev graf, takoj dobimo naslednjo trditev:

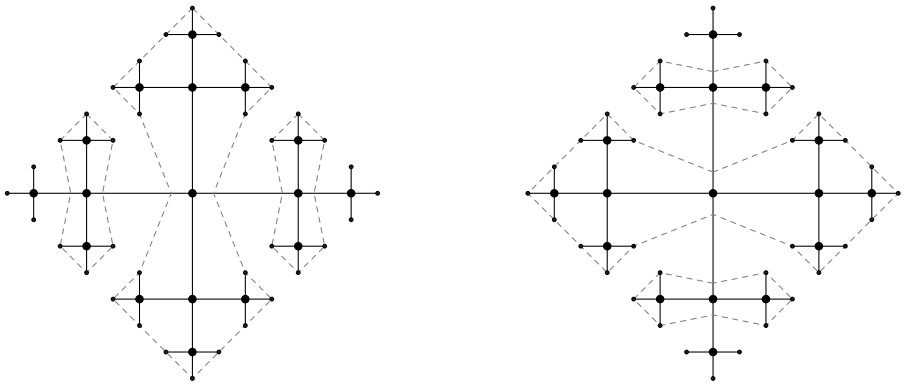
Trditev 5.10. *Na prosto grupo $\mathbb{F}_2$ lahko gledamo kot na grupo simetrij regularnega drevesa $\mathcal{T}_4$.*

Grupa $\mathbb{F}_2$ deluje na $\mathcal{T}_4$ z leve strani. Generator a pošlje vozlišče, ki predstavlja reducirano besedo ω, v vozlišče, ki je v korespondenci z reducirano besedo, ki je ekvivalentna besedi $a \cdot \omega$. Zapišimo še formulo za to delovanje. Naj bo ω enaka $\omega = \alpha\omega'$, kjer je α samo ena črka. Delovanje generatorja a je dano z

$$a \cdot \omega = a \cdot \alpha \cdot \omega' = \begin{cases} a\omega, & \text{če} \quad a^{-1} \neq \alpha, \\ \omega', & \text{če} \quad a^{-1} = \alpha. \end{cases}$$

Delovanje $a \in \mathbb{F}_2$ na drevo $\mathcal{T}_4$ je nekakšen premik v desno. Da bi to preverili, obravnavajmo podgraf drevesa $\mathcal{T}_4$, podanega z vozlišči, ki so v korespondenci z $\{a^n \mid n \in \mathbb{Z}\}$. Množenje z leve z generatorjem a potisne kombinatorično premico za eno enoto v desno, posledično se premakne tudi celoten Cayleyjev graf, kot je to prikazano na sliki 44a.

Delovanje generatorja b je podobno. Glavna razlika je v tem, da kombinatorično premico, ki je dana z vozlišči $\{b^n \mid n \in \mathbb{Z}\}$, premakne za eno enoto gor. Tudi to je prikazano na sliki 44b.



(a) Množenje z leve z generatorjem a premakne navpične cvetne liste v desno.

(b) Množenje z leve z generatorjem b premakne vodoravne cvetne liste gor.

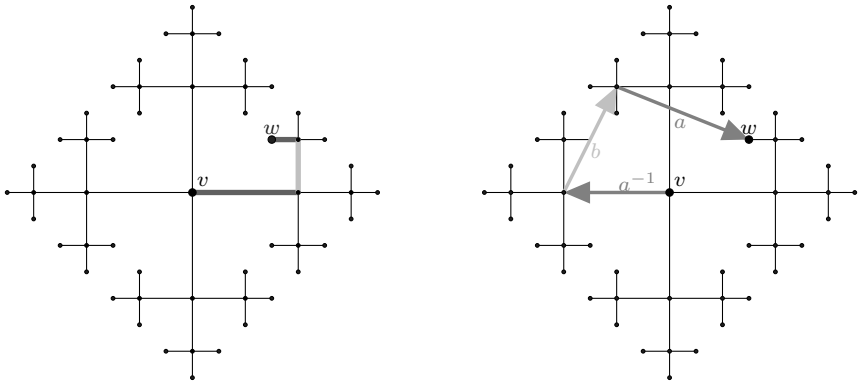
Slika 44: Delovanje generatorjev a in b na Cayleyjev graf proste grupe $\mathbb{F}_2$.

Na tem mestu bi se bilo dobro spomniti, da vizualiziranje delovanja danega elementa v grupi G na njen Cayleyjev graf, ni enako, kot slediti potem od identitete do danega elementa v Cayleyjevem grafu.

Poglejmo si to na konkretnem primeru. Imamo pot povezav med vozliščem v, ki je v korespondenci z identiteto, in vozliščem w, ki se nahaja v Cayleyjevem grafu grupe $\mathbb{F}_2$. Ta pot je prikazana na sliki 45a. Pot povezav je označena z besedo aba^{-1}.

Zmotno bi bilo, če bi domnevali, da ta pot sledi gibanju vozlišča v pod delovanjem teh treh transformacij.

Na sliki 45b je prikazano gibanje vozlišča v pod delovanjem aba^{-1}. Delovanje grupe $\mathbb{F}_2$ je levo delovanje, torej najprej na vozlišču v uporabimo transformacijo a^{-1}. S tem vozlišče v prestavimo v levo. Potem uporabimo b na vozlišču $a^{-1} \cdot v$ in na koncu še a na vozlišču $ba^{-1} \cdot v$.



(a) Pot povezav, ki povezuje vozlišči v in w v Cayleyjevem grafu grupe $\mathbb{F}_2$.

(b) Pot od vozlišča v do vozlišča w glede na delovanje grupe $\mathbb{F}_2$.

Slika 45: Vizualiziranje delovanja besede aba^{-1} v grupi $\mathbb{F}_2$ na njen Cayleyjev graf ni enako, kot slediti poti v grafu od v do w.

Čeprav je končni rezultat enak, pa se pot, ki jo prepotuje vozlišče v, razlikuje od poti, ki pripada besedi aba^{-1}.

5.4 Proste grupe in delovanja na drevesa

Sledeči rezultat karakterizira proste grupe preko delovanj na drevesa. Prav tako nam omogoči vpogled v naravo prostih grup in prinese uporaben pristop za dokazovanje rezultatov, kot je Nielsen-Schreierjev izrek, ki ga bomo dokazali v naslednjem razdelku.

Izrek 5.11. *Grupa G je prosta, če in samo če deluje prosto na drevo.*

V razdelku, kjer smo govorili o fundamentalnih domenah in množicah generatorjev, smo dokazali, da če grupa deluje na graf, potem obstaja fundamentalna domena za to delovanje. Na hitro se spomnimo konstrukcije te fundamentalne domene v kontekstu grupe G, ki deluje prosto na drevo $\mathcal{T}$.

Začnimo z vozliščem $v \in \mathcal{T}$ in obravnavajmo poddrevesa $\mathcal{C} \subset \mathcal{T}$, za katere velja:

1. $v \in \mathcal{C}$ in
2. če sta x in y različni si vozlišči v $\mathcal{C}$, potem ne obstaja tak element grupe $g \in G$, da bi veljalo $g \cdot x = y$.

Obstaja vsaj eno maksimalno poddrevo, ki zadošča tema dvema pogojema, letega bomo označili z $\mathcal{M}$. Ker je delovanje grupe G prosto, poddrevo $\mathcal{M}$ še ne tvori fundamentalne domene, saj slika $\mathcal{M}$ po delovanje grupe G vsebuje vsako vozlišče drevesa $\mathcal{T}$, ne vsebuje pa vsake povezave drevesa. Za vsako povezavo $e \nsubseteq \mathcal{M}$, kjer je $e \cap \mathcal{M} \neq \emptyset$, naj bo h_e zaprta polovica povezave e, ki je povezana z $\mathcal{M}$. Definirajmo množico $\mathcal{F}$ kot unijo $\mathcal{M}$ in teh polovičnih povezav. Dokaz leme 3.62 poda in dokaže spodnjo lemo:

Lema 5.12. *Pomnožica $\mathcal{F} \subset \mathcal{T}$, ki ima enake lastnosti, kot so opisane zgoraj, je fundamentalna domena za delovanje grupe G na drevo $\mathcal{T}$. Množica $\mathcal{F}$ vsebuje eno vozlišče za vsako orbito vozlišč pod delovanjem grupe G.*

S pomočjo opisanega zgoraj se lotimo dokaza izreka 5.11:

Dokaz: Najprej se lotimo lažjega dela dokaza našega izreka. Če je G prosta grupa, potem deluje prosto na svoj Cayleyjev graf, ki je drevo.

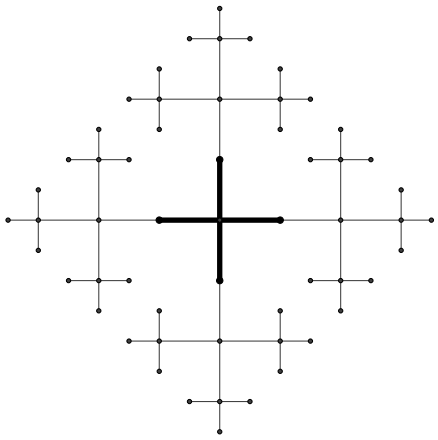
Preostane nam še dokaz v drugo smer. Domnevajmo, da G deluje prosto na drevo $\mathcal{T}$ in da je $\mathcal{F}$ taka fundamentalna domena, kot je opisana zgoraj. Za vsako polovično povezavo $h_e \in \mathcal{F}$ naj bo $g_e \in G$ tak, da je $\mathcal{F} \cap g_e \cdot \mathcal{F}$ razpolovišče povezave e. Označimo množico vseh takih g_e z oznako $\mathcal{S}$. Ker je $\mathcal{F} \cap g_e \cdot \mathcal{F}$ razpolovišče povezave, je tudi $g_e^{-1} \cdot \mathcal{F} \cap \mathcal{F}$ razpolovišče povezave. Če je torej $g_e \in \mathcal{S}$, je tudi $g_e^{-1} \in \mathcal{S}$, zato velja: če je $g_e \in \mathcal{S}$, potem obstaja taka polovična povezava $h_{\overline{e}} \in \mathcal{F}$, da je $g_e^{-1} = g_{\overline{e}}$.

Množica $\mathcal{S}$ je množica generatorjev za grupo G po izreku 3.67. Ker lahko vsak element v $\mathcal{S}$ damo v par s svojim inverzom, lahko s S označimo maksimalno podmnožico množice $\mathcal{S}$, ki ne vsebuje hkrati elementa in njegovega inverza. Zato lahko zapišemo $\mathcal{S} = S \cup S^{-1}$. Tu moramo opozoriti na to, da smo domnevali, da ne obstaja tak element grupe $g \in G$, da je $g = g^{-1}$. Z drugimi besedami, domnevali smo, da v grupi G ne obstaja element reda 2. To pa lahko domnevamo zaradi izreka 5.5.

Fiksirajmo vozlišče $v \in \mathcal{M}$ in za vsak $g_e \in S \cup S^{-1}$ označimo s $\mathcal{T}_e$ poddrevo drevesa $\mathcal{T}$, ki je inducirano s takšno množico vozlišč $v' \in \mathcal{T} \setminus \mathcal{M}$, da reducirana pot od v do v' prečka polovično povezavo h_e. Poddrevo $\mathcal{T}_e$ lahko ekvivalentno definiramo kot maksimalno poddrevo, vsebovano v $\mathcal{T} \setminus \mathcal{M}$, ki si deli vozlišče s povezavo e.

Zgled 5.13. Za lažjo predstavo se spomnimo na delovanje grupe $\mathbb{F}_2$ na njen Cayleyjev graf. V tem primeru je $\mathcal{M}$ le eno vozlišče in fundamentalna domena $\mathcal{F}$ sestoji iz tega vozlišča ter štirih polovičnih povezav. Množica S bo sestavljena iz dveh

elementov in štiri poddrevesa $\mathcal{T}_e$ bodo maksimalna poddrevesa, vsebovana v povezanih komponentah, ki nastanejo po odstranitvi fundamentalne domene $\mathcal{F}$. To je prikazano na sliki 46.



Slika 46: Fundamentalna domena za delovanje proste grupe $\mathbb{F}_2$ na svoj Cayleyjev graf izgleda kot nekakšen križ iz štirih polovičnih povezav.

Pri nadaljevanju dokaza si pomagajmo s Ping-pong lemo. Z njeno pomočjo bomo dokazali, da je G prosta grupa z bazo S. Uporabimo zapis, ki se uporablja v omenjeni lemi:

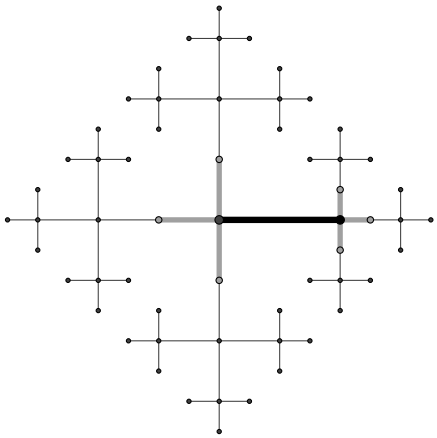
- za vsak $g_e \in \mathcal{S}$ naj bo $X_{\mathcal{S}}$ pripadajoče poddrevo $\mathcal{T}_e$;
- vzemimo $p = v \in \mathcal{M}$ za točko, ki je zunaj unije poddreves $\bigcup \mathcal{T}_e$.

Prvi pogoj Ping-pong leme sledi iz definicije poddreves $\mathcal{T}_e$. Naj bo $g_e \in S$ in naj bo $\mathcal{T}_{e'}$ eno od poddreves, kjer $g_{e'} \neq g_e^{-1}$. Naj bo $\overline{e} = g_e^{-1} \cdot e$, ki označuje povezavo, ki povezuje $g_e^{-1}(\mathcal{M})$ in $\mathcal{M}$. Za poljubno vozlišče $w \in \mathcal{T}_{e'}$ obstaja minimalna pot povezav, ki povezuje $g_e^{-1} \cdot v$ in w. Če na tej poti uporabimo g_e, dobimo minimalno pot povezav od vozlišča v do vozlišča $g_e \cdot w$. Prvotna pot je prečkala $\overline{e} = g_e^{-1} \cdot e$, zato bo slika poti pod g_e šla preko povezave e. Torej je po konstrukciji $g_e \cdot w \in \mathcal{T}_e$. Ker je bilo w poljubno vozlišče poddrevesa $\mathcal{T}_{e'}$, je $g_e(\mathcal{T}_{e'}) \subset \mathcal{T}_e$, kar izpolnjuje tudi drugi pogoj Ping-pong leme. S pomočjo Ping-pong leme smo torej dokazali, da je G prosta grupa. ∎

Dokaz izreka 5.11 je konstruktiven, zato nam ponudi tudi metodo za iskanje baze za grupo G.

Zgled 5.14. Obravnavajmo sodo podgrupo H proste grupe $\mathbb{F}_2$, kjer je množica $\{a, b\}$ baza proste grupe $\mathbb{F}_2$. Podgrupa H je sestavljena iz vseh elementov grupe $\mathbb{F}_2$, ki so sode dolžine. Soda podgrupa H deluje na Cayleyjev graf grupe $\mathbb{F}_2$, ki je regularno drevo $\mathcal{T}_4$. Začnimo konstrukcijo $\mathcal{M}$ z izbiro vozlišča, ki je asociiran z

identiteto. Ker potrebujemo še vozlišče, ki predstavlja elemente lihe dolžine, dodamo v $\mathcal{M}$ še vozlišče, ki je asociirano z a. Povezava e, ki povezuje izbrani vozlišči, zaključi konstrukcijo $\mathcal{M}$. Fundamentalna domena $\mathcal{F}$ sestoji iz te povezave e in šestih polovičnih povezav, ki so si sosednja s povezavo e. Oglejmo si to na sliki 47.



Slika 47: Na sliki je odebeljeno in s črno barvo označen podgraf $\mathcal{M}$, ki je sestavljen iz povezave e in dveh vozlišč, s sivo barvo pa so označeni še deli, ki jih je potrebno dodati v fundamentalno domeno za delovanje sode podgrupe H na Cayleyjev graf grupe $\mathbb{F}_2$.

Ker imamo v fundamentalni domeni $\mathcal{F}$ šest polovičnih povezav, lahko takoj sklepamo, da bo naša iskana baza imela tri elemente. Da bi poiskali elemente, ki se nahajajo v bazi, moramo najti vse $g \in H$, za katere velja $g \cdot \mathcal{F} \cap \mathcal{F} \neq \emptyset$. Celoten seznam elementov, ki temu pogoju ustrezajo, izgleda kot $\{a^2, a^{-2}, ab, b^{-1}a^{-1}, ab^{-1}, ba^{-1}\}$. Ko iz množice odstranimo inverze, pa seznam izgleda kot $\{a^2, ab, ab^{-1}\}$. Dobljena množica predstavlja bazo za sodo podgrupo H proste grupe $\mathbb{F}_2$.

5.5 Nielsen-Schreierjev izrek

Zaključimo z osupljivim rezultatom o prostih grupah, ki ga je leta 1921 prvi dokazal Jakob Nielsen za končno generirane proste grupe. Njegov dokaz je nekaj let kasneje razširil na vse proste grupe Otto Schreier.

Posledica 5.15 (Nielsen-Schreierjev izrek)**.** *Vsaka podgrupa proste grupe je prosta.*

Dokaz: Naj bo H podgrupa proste grupe $\mathbb{F}$. Grupa $\mathbb{F}$ deluje prosto na svoj Cayleyjev graf, ki je drevo. Posledično tudi podgrupa H deluje prosto na to drevo. Po karakterizaciji prostih grup, ki je dana z izrekom 5.11, je H prosta grupa. ∎

Literatura

[1] Mark Anthony Armstrong, *Groups and symmetry*, Springer-Verlag, New York, 1988.

[2] Lowell W. Beineke, Robin J. Wilson, Peter J. Cameron, *Topics in algebraic graph theory*, Cambridge university press, Cambridge, 2004.

[3] Alexandre V. Borovik, Formal languages and their application to combinatorial group theory, v: *Groups, languages, algorithms: AMS-ASL Joint Special Session on Interactions between Logic, Group Theory and Computer Science, January 16–19, 2003, Baltimore, Maryland*, American Mathematical Society, Providence, 2005.

[4] Matt Day, *Notes on Cayley graphs for math 5123*, [ogled 15. 2. 2015], dostopno na `http://comp.uark.edu/~matthewd/5123/cayleygraphs.pdf`.

[5] John B. Fraleigh, *A first course in abstract algebra*, Addison-Wesley, Boston, 2003.

[6] Ashwin Ganesan, *Automorphism groups of graphs*, verzija 26. 6. 2012, [ogled 1. 2. 2015], dostopno na `http://arxiv.org/pdf/1206.6279.pdf`.

[7] Martin Juvan, Primož Potočnik, *Teorija grafov in kombinatorika: primeri in rešene naloge*, Društvo matematikov, fizikov in astronomov Slovenije, Ljubljana, 2000.

[8] Elena Konstantinova, *Lecture notes on some problems on Cayley graphs*, Knjižnica za tehniko, medicino in naravoslovje, Koper, 2012.

[9] Clara Löh, *Geometric group theory, an introduction*, Universitaet Regensburg, Regensburg, 2011.

[10] John Meier, *Groups, graphs and Trees. An introduction to the geometry of infinite groups*, London Mathematical Society Student Texts **73**, Cambridge University Press, Cambridge, 2008.

[11] Jean-Pierre Serre, *Trees*, Springer-Verlag, Berlin Heidelberg, 1980.

[12] Ivan Vidav, *Algebra*, Društvo matematikov, fizikov in astronomov Slovenije, Ljubljana, 2003.

[13] Samuel White, The group generated by $x \to x + 1$ and $x \to x^p$ is free, *Journal of Algebra* **118** (1988), 408–422.