Proste grupe in drevesa
Seminar

Jakob Pogačnik Souvent
Fakulteta za matematiko in fiziko
Oddelek za matematiko

22. maj 2022

1 Uvod

V študiju algebraičnih struktur imajo poseben pomen strukture, ki jih lahko opišemno z neko množico generatorjev, ki so med seboj čim manj povezani. To so t.i. **proste** strukture.

V vektorskoh prostorih, denimo, nepovezanost elementov pojmujemo kot njihovo linearno neodvisnost. In ker ima vsak končnorazsežni vektorski prostor bazo iz linearno neodvisnih vektorjev, ima kot tak, obliko proste strukture.

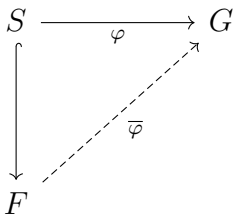
V članku se bomo ukvarjali predvsem s problemom prepoznavanja prostih struktur znotraj teorije grup. Izkaže se namreč, da za razliko od vektorskih prostorov, nima vsaka grupa oblike proste strukture, kar je eden izmed razlogov, zakaj je teorija grup nekoliko bolj zapletena kot študij vektorskih prostorov.

2 Proste grupe

Preden se lahko lotimo problema iskanja prostih struktur v teoriji grup, rabimo najprej postaviti definicijo **proste grupe**.

Definicija 1 (Prosta grupa)**.** *Naj bo S množica. Za grupo F, ki vsebuje S Pravimo, da S* ***prosto generira*** *F, če velja:*

Za vsako grupo G in vsako preslikavo $\varphi : S \longrightarrow G$ obstaja enoličnо določen homomorfizem $\overline{\varphi} : F \longrightarrow G$, ki razširi φ.



*Grupi F pravimo **prosta**, če vsebuje kakšno podmnožico, ki jo prosto generira, zgornji lastnosti pa pravimo **univerzalna lastnost prostih grup**.*

Če imamo pri branju zgornje definicije v mislih analogijo z vektorskimi prostori, lahko na elemente množice S gledamo kot na bazne vektore. Univerzalna lastnost nam potem pove, da je homomorfizem proste grupe enolično definiran s slikami "baznih vektorjev".

Opomba 1. *V definiciji ne zahtevamo, da je množica S množica generatorjev grupe F, vendar bomo videli, da to sledi iz zahtevane univerzalne lastnosti (glej Izrek 3).*

Da utrdimo pojem proste grupe, si oglejmo nekaj zgledov.

Zgled 1.

1. *Trivialna grupa je prosto generirana s prazno množico.*

2. *$\mathbb{Z}$ je prosta grupa.*

   Pri dokazu da $\mathbb{Z}$ je prosta grupa je dovolj, da najdemo neko množico ki jo prosto generira. Denimo $S := \{1\}$. Vzemimo poljubno preslikavo $\varphi : S \longrightarrow G$, kjer je G poljubna grupa. Če $\varphi(1) = e$ je trivialni homomorfizem $\overline{\varphi}(n) = e$ ustrezna razširitev. Če pa $\varphi(1) = g_0 \neq e$ predpis $\overline{\varphi}(n) = g_0^n$ ustrezno razširi φ.

   Omembe vredno je, da univerzalne lastnosti ne izpolnjuje vsaka podmnožica proste grupe. Niti je ne izpolnjuje vsaka podmnožica generatorjev. Če bi naprimer vzeli $S := \{2, 3\}$ za preslikavo $\varphi : S \longrightarrow \mathbb{Z}_2$ definirano kot $\varphi(2) = 1$ in $\varphi(3) = 1$ ne obstaja homomorfizem ki na S sovpada s φ. Če bi namreč obstajala razširitev $\overline{\varphi}$, bi moralo veljati

   $$\overline{\varphi}(1) = \overline{\varphi}(3 - 2) = \overline{\varphi}(3) - \overline{\varphi}(2) = 1 - 1 = 0,$$

   kar pa vodi v protislovje, ker

   $$\overline{\varphi}(2) = \overline{\varphi}(1 + 1) = \overline{\varphi}(1) + \overline{\varphi}(1) = 1 + 1 = 0 \neq 1 = \varphi(2).$$

3. *$\mathbb{Z}_2$ ni prosto generirana.*

   Za $\mathbb{Z}_2$ imamo samo 3 možne kandidate za množico S. To so $S_1 = \{0\}$, $S_2 = \{0, 1\}$ in $S_3 = \{1\}$. Hitro se prepričamo, da S_1 in S_2 nista ustrezna, saj lahko v tem primeru za preslikavo φ izberemo tako preslikavo v netrivialno grupo G, ki 0 ne slika v enoto. Ker homomorfizem slika enoto φ torej ne moremo razširiti do homomorfizma. Opazimo, da množica S, ki prosto generira grupo F, ne more vsebovati enote.

   Poiščimo še protiprimer za S_3. Definirajmo preslikavo $\varphi : S_3 \longrightarrow \mathbb{Z}$ s predpisom $\varphi(1) = 2$. Če obstaja $\overline{\varphi}$ ki na S sovpada s φ mora veljati

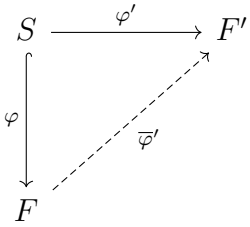
$$\overline{\varphi}(0) = \overline{\varphi}(1 + 1) = \overline{\varphi}(1) + \overline{\varphi}(1) = 2 + 2 = 4$$

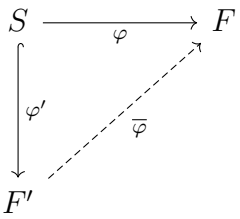
   kar pa je protislovje, saj mora homomorfizem slikati enoto v enoto.

Oglejmo nekaj osnovnih lastnosti prostih grup, ki jih bomo potrebovali v kasnejših dokazih.

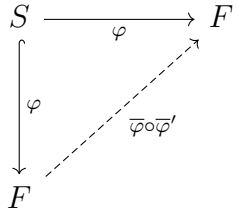
Izrek 1 (Enoličnost prostih grup)**.** *Naj bo S množica. Potem do izomorfizma natančno obstaja največ ena grupa prosto generirana z S.*

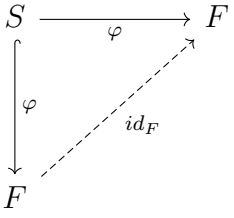
Dokaz. Naj bosta F in F' grupi, prosto generirani z množico S. Naj bosta $\varphi : S \hookrightarrow F$ in $\varphi' : S \hookrightarrow F'$ inkluziji. Po univerzalni lasnosti prostih grup lahko φ in φ' razširimo do homomorfizmov $\overline{\varphi}$ in $\overline{\varphi'}$.





Kompozitum homomorfizmov $\overline{\varphi} \circ \overline{\varphi}' : F \to F$ je homomorfizem, ki je na S identiteta ($\overline{\varphi}$ in $\overline{\varphi}'$ na S sovpadata z φ in φ'). Če na φ gledamo kot na preslikavo iz S v F sta torej tako $\overline{\varphi} \circ \overline{\varphi}'$ kot id_F razširitvi, ki ustrezata univerzalni lastnosti in zato po enoličnosti razširitve velja $\overline{\varphi} \circ \overline{\varphi}' = id_F$.





Podobno $\overline{\varphi}' \circ \overline{\varphi} = id_{F'}$, torej je $\overline{\varphi} \circ \overline{\varphi}'$ izomorfizem. □

Izrek 2 (Eksistenca prostih grup)**.** *Naj bo S množica. Potem obstaja grupa, prosto generirana z S.*

Opomba 2. *Po izreku 1 je ta grupa enolično določena do izomorfizma natančno.*

Dokaz. Ideja dokaza je konstrukcija grupe sestavljene iz t.i. *besed*, ki so sestavljene iz elementov množice S in njihovih inverzov, na katerih bomo uporabili le neposredno pravilo krajšanja.

Konkretno definiramo

$$A := S \cup \widehat{S}$$

kot abecedo iz katere bomo sestavili naše besede. Tu $\widehat{S} = \{\widehat{s} \mid s \in S\}$ predstavlja disjunktno kopijo S (t.j. $\widehat{\cdot} : S \longrightarrow \widehat{S}$ je bijekcija in $S \bigcap \widehat{S} = \emptyset$), ki bo v konstrukciji prevzela vlogo inverzov.

V prvem koraku vzemimo z oznako A^* množico vseh končnih zaporedij iz abecede A. To vsebuje, med drugimi, tudi prazno besedo ε. Na A^* definirajmo binarno operacijo kompozicije, ki stakne skupaj dve besedi. Ta operacija je asociativna in ε je nevtralni element.

V nadaljevanju definirajmo

$$F(S) := A^*/\sim$$

kjer je $\sim$ ekvivalenčna relacija, definirana kot

$$\forall x, y \in A^* \; \forall s \in S : xs\widehat{s}y \sim xy$$
$$\forall x, y \in A^* \; \forall s \in S : x\widehat{s}sy \sim xy.$$

Drugače, elementa v A^* obravnavamo kot ekvivalentna, če se razlikujeta natanko za neposredno uporabo pravila krajšanja (Opomba: popolnoma formalno za $\sim$ vzamemo najmanjšo ekvivalenčno relacijo, ki zadostuje zgornjemu pogoju).

Ni težko preveriti, da kompozicija besed v A^* inducira dobro definirano binarno operacijo $\cdot : F(S) \times F(S) \longrightarrow F(S)$ definirano kot

$$[x] \cdot [y] = [xy]$$

kjer so z oglatimi oklepaji označeni ekvivalenčni razredi po $\sim$.

Pokažimo, da je množica $F(S)$ s tako operacijo grupa. Očitno je $[\varepsilon]$ nevtralni element, asociativnost pa sledi iz asociativnosti kompozicije v A^*. Induktivno (po dolžini besede) definiramo preslikavo $I : A^* \longrightarrow A^*$, ki besedi priredi inverz kot

$$I(\varepsilon) = \varepsilon$$
$$I(sx) := I(x)\widehat{s}$$
$$I(\widehat{s}x) := I(x)s$$

za vse $x \in A^*$ in $s \in S$. Induktivno vidimo da $I(I(x)) = x$ in

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

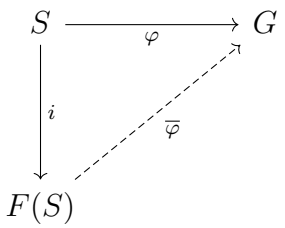
za vse $x \in A^*$ (zadnja enakost sledi iz definicije $\sim$). Zato tudi

$$[x] \cdot [I(x)] = [I(I(x))] \cdot [I(x)] = [\varepsilon].$$

Torej je $F(S)$ grupa.

Ostane name le še pokazati, da S prosto generira $F(S)$. Naj bo $i : S \longrightarrow F(S)$ preslikava, ki vsaki črki $S \subset A^*$ priredi njen ekvivalenčni razred v $F(S)$. Po konstrukciji je $i(S)$ množica generatorjev $F(S)$.

Zdaj pokažimo, da ima $F(S)$ naslednjo lastnost, podobno univerzalni lastnosti prostih grup: za vsako grupo G in preslikavo $\varphi : S \longrightarrow G$ obstaja enolično določen homomorfizem grup $\overline{\varphi} : F(S) \longrightarrow G$, da $\varphi = \overline{\varphi} \circ i$.



Opomnimo, da formalno gledano to ni univerzalna lastnost prostih grup, saj grupa $F(S)$ ne vsebuje množice S, temveč njej ustrezne ekvivalenčne razrede $i(S)$. Če je i injektivna, pa lahko S identificiramo z $i(S)$ in to res postane univerzalna lastnost.

Pri dokazu zgornje lastnosti z danim φ induktivno definiramo

$$\begin{aligned} \varphi^* : A^* &\longrightarrow G \\ \varepsilon &\longmapsto e \\ sx &\longmapsto \varphi(s) \cdot \varphi^*(x) \\ \widehat{s}x &\longmapsto (\varphi(s))^{-1} \cdot \varphi^*(x) \end{aligned}$$

za vse $s \in S$ in vse $x \in A^*$. Lahko je videti, da je φ^* kompatibilna z ekvivalenčno relacijo $\sim$ in da $\varphi^*(xy) = \varphi^*(x) \cdot \varphi^*(y)$. Torej φ^* inducira dobro definiran homomorfizem

$$\begin{aligned} \overline{\varphi} : F(S) &\longrightarrow G \\ [x] &\longmapsto [\varphi^*(x)]. \end{aligned}$$

Po konstrukciji je $\varphi = \overline{\varphi} \circ i$. Ker $i(S)$ generira $F(S)$, pa je $\overline{\varphi}$ enolično določen.

Ostane nam le še dokaz injektivnosti i. Naj bosta $s_1, s_2 \in S$ in $\varphi : S \longrightarrow \mathbb{Z}$ poljubna preslikava, da velja $\varphi(s_1) = 1$ in $\varphi(s_2) = -1$. Potem nam inducirani $\overline{\varphi}$ da

$$\overline{\varphi}(i(s_1)) = \varphi(s_1) = 1 \neq -1 = \varphi(s_2) = \overline{\varphi}(i(s_2)).$$

Oziroma $i(s_1) \neq i(s_2)$.

Torej je i injektivna in lahko S identificiramo z njegovo sliko $i(S)$, zgornja lastnost pa tako res postane univerzalna lastnost prostih grup. □

Izrek 3. *Naj bo F grupa, prosto generirana z S. Potem je S množica generatorjev grupe F.*

Dokaz. Po konstrukciji trditev velja za prosto grupo $F(S)$, ki je generirana z S (glej dokaz izreka 2). Po izreku o enoličnosti prostih gruop (glej izrek 1), obstaja izomorfizem med $F(S) \cong F$, ki je na S identiteta, iz česar sledi, da je S množica generatorjev grupe F. □

Ker je formalno delo s kvocientno grupo, ki smo jo dobili pri konstrukciji v izreku 2, nekoliko zamudno in težje razumljivo, brez dokaza privzemimo naslednjo trditev, ki nam bo nudila ekvivalentno reprezentacijo grupe, prosto generirane s poljubno množico S.

Če bralca zanima dokaz, naj se obrne na dokaz trditve 3.3.5 v članku [1].

Definicija 2 (Okrajšana beseda)**.** *Naj bo S množica in $(S \cup \widehat{S})^*$ množica vseh besed nad elementi S in njihovimi formalnimi inverzi. Naj bo $n \in \mathbb{N}$ in $s_1, \ldots, s_n \in S \cup \widehat{S}$. Za besedo $s_1 \ldots s_n$ pravimo, da je **okrajšana**, če velja*

$$s_{j+1} \neq \widehat{s}_j \quad in \quad \widehat{s}_{j+1} \neq s_j$$

za vse $j \in \{1, \ldots, n-1\}$. Posebej: ε je okrajšana.

Množico vseh okrajšanih besed v $(S \cup \widehat{S})^*$ označimo z $F_{red}(S)$.

Trditev 1. *Naj bo S množica.*

1. *Množica okrajšanih besed $F_{red}(S)$ nad $S \cup \widehat{S}$ tvori grupo za operacijo kompozicije, definirano kot*

$$F_{red}(S) \times F_{red}(S) \longrightarrow F_{red}(S)$$
$$(s_1 \ldots s_n, s_{n+1} \ldots s_m) \longmapsto (s_1 \ldots s_{n-r} s_{n+1+r} \ldots s_m)$$

   kjer so $s_1, \ldots, s_m \in S \cup \widehat{S}$ in je r največje tako število, da za vsak $j \in \{0, \ldots, r-1\}$ velja

$$s_{n-j} = \widehat{s}_{n+1+j} \quad ali \quad \widehat{s}_{n-j} = s_{n+1+j}.$$

   Z drugimi besedami, kompozicija je definirana s konkatinacijo dveh besed in nato okrajšavo največjega možnega števila elementov na mestu konkatinacije.

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

Množico $F_{red}(S)$ torej dobimo tako, da se v $F(S)$ omejimo na enega predstavnika vsakega ekvivalenčnega razreda. To nam nekoliko okrajša delo v nadaljnjih izrekih, saj smo delo z ekvivalenčnimi razredi prevedli na delo s predstavnikom, kar nam v dokazih prihrani dokaz dobre definiranosti lastnosti oz. operacij na ekvivalenčnih razredih.

3 Cayleyjevi grafi

Eno izmed temeljnih vprašanj v teoriji grup je, kako si grupe predstavljati kot geometrijske objekte. Eden izmed načinov, kako to storimo, je z uporabo cayleyevih grafov, ki opišejo relacije med elementi grupe glede na njeno množico generatorjev.

Preden definiramo cayleyeve grafe, zapišimo še definiciji za pot in cikel v grafu. V cayleyevih grafih bodo vlogo vozlišč zavzeli elementi grupe, vlogo povezav pa relacije med njimi, zato je koristno, da privzamemo tako definicijo poti in ciklov, ki nam bo izolirala elemente grupe.

Definicija 3 (Pot)**.** ***Pot*** *ki povezuje vozlišči v_0 in v_n v grafu $X = (V, E)$, je zaporedje paroma različnih vozlišč $v_0, \ldots, v_n \in V$, za katerega velja, da je $\{v_i, v_{i+1}\} \in E$ za vsak $i \in \{0, \ldots, n-1\}$.*

Definicija 4 (Cikel)**.** *Naj bo $n \in \mathbb{N}$, $n > 2$.* ***Cikel*** *v grafu $X = (V, E)$ dolžine n je pot $v_0, \ldots, v_n$ v X, za katero velja $\{v_{n-1}, v_n\} \in E$.*

Definicija 5 (Cayleyev graf)**.** *Naj bo S podmnožica, ki generira grupo G.* ***Cayleyjev graf*** *G glede na množico generatorjev S je graf $Cay(G, S)$, katerega množica vozlišč je množica G in katerega množica povezav je množica*

$$\{\{g, g \cdot s\} \mid g \in G, s \in (S \cup S^{-1}) \setminus \{e\}\},$$

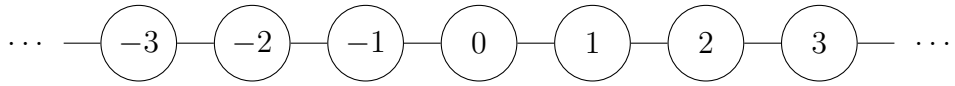
kjer je $s \cdot$ označeno množenje v grupi G.

Dve vozlišči v Cayleyjevem grafu sta si torej sosednji natanko tedaj, ko se razlikujeta le za desno množenje z elementom (ali inverzom) dane množice S.

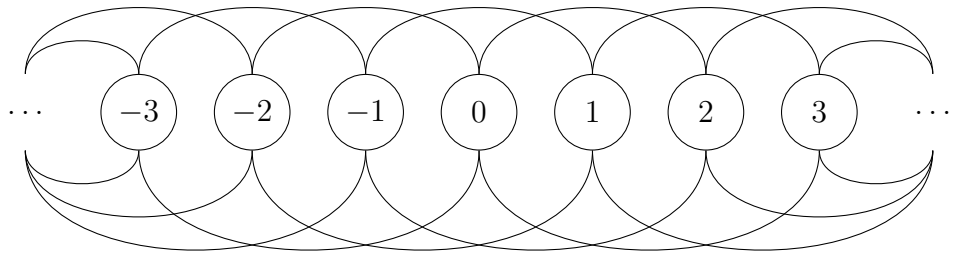
Za boljšo predstavo si oglejmo cayleyeve grafe nekaterih nam že znanih grup.

Zgled 2. *Cayleyevi grafi nekaterih dobro znanih grup.*

1. $Cay(\mathbb{Z}, \{1\})$

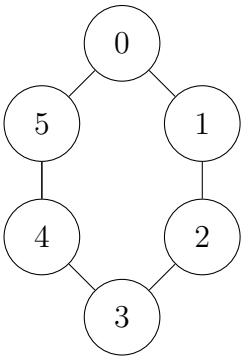


2. $Cay(\mathbb{Z}, \{2, 3\})$



Vidimo, da cayleyev graf ni odvisen le od grupe, temveč tudi od množice generatorjev ki jo vzamemo.

3. $Cay(\mathbb{Z}_6, \{1\})$

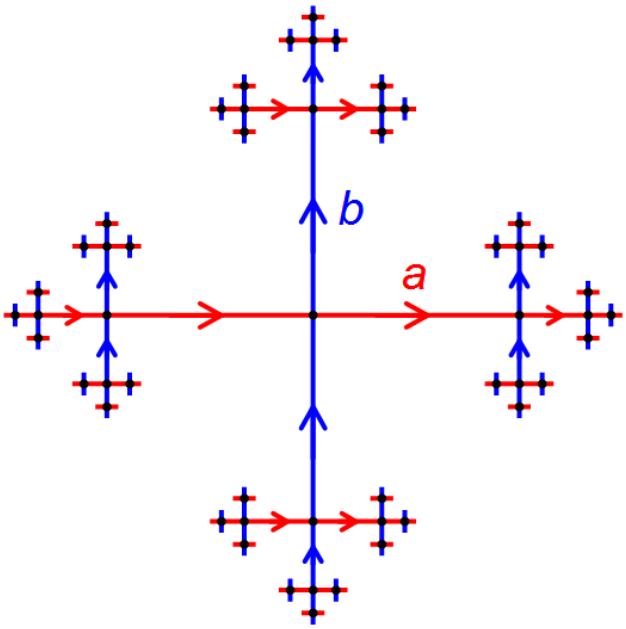


Seveda pa nas v tem članku ne zanimajo katerekoli grupe, temveč proste grupe. Naravno se torej porodi vprašanje, kako izgleda cayleyev graf proste grupe glede na množico, ki jo prosto generira (po izreku 3 ta množica generira grupo)? Povezave v cayleyevim grafu namreč predstavljajo relacije med elementi grupe, glede na množico generatorjev, v prostih grupah pa generatorji med seboj nimajo relacij.

Če torej poskusimo skicirati graf neke proste grupe dobimo skico podobno sliki 1. Opazimo, da se odsotnost relacij med generatorji v grafu izraža kot odsotnost povezav med elementi, kar porodi najmanjši možen povezan graf, drevo.

Našo ugotovitev zapišemo v izrek in jo tudi formalno dokažemo.

Izrek 4. *Naj bo F grupa, prosto generirana z $S \subset F$. Potem je graf $Cay(F, S)$ drevo.*



Slika 1: Cayleyev graf proste grupe $Cay(F_{red}(S), \{a, b\})$

Dokaz. Brez škode za splošnost se omejimo na $F_{red}(S)$, saj sta $F \cong F_{red}(S)$ izomorfna. Če imamo v grafu $Cay(F_{red}(S), S)$ cikel, to pomeni, da lahko začnemo v nekem vozlišču x in z zaporednim množenjem z elementi S (elementa sta sosednja natanko tedaj ko se razlikujeta za množenje z nekim elementom S) pridemo nazaj v x. Torej

$$xs_1 \dots s_n = x.$$

Okrajšamo x in dobimo

$$s_1 \dots s_n = \varepsilon,$$

kar pa je protislovno, saj je v $F_{red}(S)$ to možno natanko tedaj, ko so si ustrezni sosedni elementi inverzni (inverz pa pomeni potovanje po isti povezavi v obratno smer s čimer pridemo v protislovje z enoličnostjo vozlišč v ciklu). □

Opomba 3. *Obrat v splošnem ne drži, t.j. ni res da za vsak $Cay(F, S)$ sledi, da je F prosto generirana z S. Protiprimer bi bil denimo $Cay(\mathbb{Z}_2, \{1\})$.*

Kljub temu pa lahko pridemo do obrata, če poleg drevesne strukture dodamo predpostavko, da se nobena elementa množice S ne zmnožita v enoto. Tako se izognemo primerom, ko bi ustvarili cikel dolžine 2, kar nam v posebnih primerih (kot $Cay(\mathbb{Z}_2, \{1\})$ zgoraj), ker v povezavah ne ločimo usmerjenosti, ustvari graf, ki ustreza definiciji drevesa.

Izrek 5 (Obrat)**.** *Naj bo G grupa in naj bo $S \subset G$ množica generatorjev G. Dodatno naj velja, da $s \cdot t \neq e$ za vsaka $s, t \in S$.*

Če je Cayleyev graf $Cay(G, S)$ drevo, potem S prosto generira G.

Dokaz. Naj bo G grupa in $S \subset G$ taka da, velja predpostavka izreka. Da pokažemo, da je G prosto generirana, je dovolj, da pokažemo, da je G izomorfna $F_{red}(S)$ z izomorfizmom, ki je na S identiteta.

Ker je $F_{red}(S)$ prosto generirana z S nam univerzalna lastnost prostih grup že nudi obetavnega kandidata za izomorfizem, t.j. homomorfizem $\overline{\varphi}$, ki ga dobimo z razširitvijo identitete $\varphi : S \longrightarrow G$. Ker je po predpostavki S množica generatorjev G, hitro sledi, da je $\overline{\varphi}$ surjektiven.

Predpostavimo da $\overline{\varphi}$ ni injektiven. Potem obstajata neka $s_1 \dots s_n \in F_{red}(S) \setminus \{\varepsilon\}$, kjer $s_1, \dots, s_n \in S \cup \widehat{S}$, ki se slika v enoto $\overline{\varphi}(s_1 \dots s_n) = e$ (identificiramo sliki dveh različnih besed in obe strani množimo z inverzi črk. Ker sta besedi različni dobimo neprazno besedo ki se slika v enoto). Ker je $\overline{\varphi}$ homomorfizem sledi $s_1 \dots s_n = e$.

Ločimo primere

1. Če bi bil $n = 1$ bi veljalo $e \in S$, kar ne more biti res (glej zgled 1).
2. Če $n = 2$ potem
$$e = s_1 s_2$$
Spomnimo se, da sta $s_1, s_2 \in S \cup \widehat{S}$. Velja ena izmed naslednjih možnosti:
   (a) Ali $s_1, s_2 \in S$, kar je v protislovju z predpostavko, da
   $$\forall s, t \in S : s \cdot t \neq e.$$
   (b) Ali $s_1, s_2 \in \widehat{S}$, od koder sledi, da $s_1 s_2 = \widehat{s}_2 \widehat{s}_1$ (produkt inverzov je inverz produkta) kar je v protislovju z predpostavko
   $$\forall s, t \in S : s \cdot t \neq e,$$
   saj sta v tem primeru $\widehat{s}_2, \widehat{s}_1 \in S$.
   (c) Ali $s_1 \in S$ in $s_2 \in \widehat{S}$, kar pa bi bilo protislovno s tem, da je $s_1 s_2$ okrajšana beseda.
3. Če $n \geq 3$ v $Cay(G, S)$ začnemo v vozlišču e ter po povezavah $s_1, \dots, s_n$ sprehodimo preko vozlišč
$$\begin{aligned} g_0 &= e \\ g_i &= g_{i-1} s_i \quad \forall i \in \{1, \dots, n\}. \end{aligned}$$

Ker je $s_1 \dots s_n$ okrajšana beseda, je to zaporedje vozlišč cikel, kar pa je protislovno s predpostavko, da je $Cay(G, S)$ drevo.

Torej je predpostavka, da $\overline{\varphi}$ ni injektiven napačna. □

4 Delovanje

Cayleyevi grafi so en način, da predstavimo obliko grupe na geometrijskem objektu. Drug način povezave grup in geometrijskih objektov pa je koncept delovanja grupe, ki povezavo med elementi grupe predstavi kot povezavo med avtomorfizmi nekega geometrijskega objekta.

Za nas so posebej zanimivi geometrijski objekti grafi. Definirajmo torej delovanje grupe na grafu.

Definicija 6 (Delovanje na grafu)**.** *Naj bo G grupa. Naj bo X graf.* ***Delovanje*** *grupe G na grafu X je homomorfizem grup $G \longrightarrow Aut(X)$.*

Z drugimi besedami, delovanje G na X vsakemu elementu $g \in G$ priredi ustrezni avtomorfizem $f_g : X \longrightarrow X$, da velja

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

za vsaka $g, h \in G$.

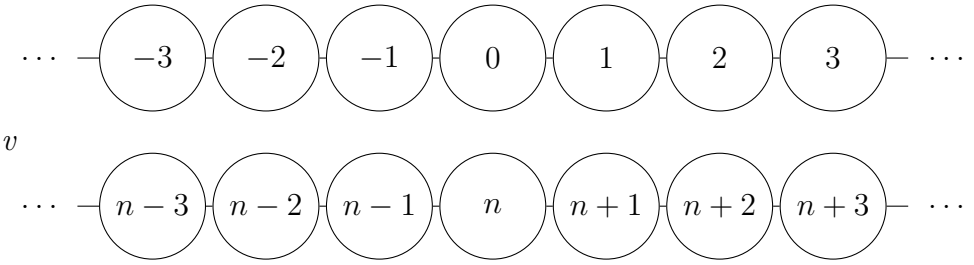
Povezava med grupo in geometrijskim objektom je posebej močna, če nanj deluje s t.i. prostim delovanjem. Ker nas v članku zanima le delovanje na grafih se tudi pri tej definiciji omejimo samo na grafe.

Definicija 7 (Prosto delovanje na grafu)**.** *Naj grupa G deluje na grafu $X = (V, E)$. Označimo delovanje kot preslikavo $\rho : G \longrightarrow Aut(X)$. To delovanje je* ***prosto****, če za vsak $g \in G \setminus \{e\}$ velja:*

$$\forall v \in V : (\rho(g))(v) \neq v, \text{ in}$$
$$\forall \{v, v'\} \in E : \{(\rho(g))(v), (\rho(g))(v')\} \neq \{v, v'\}$$

Delovanje na grafu je torej prosto, če avtomorfizem, ki je prirejen poljubnemu elementu grupe (z izjemo enote), ne fiksira nobenega vozlišča in nobene povezave; oz. če je stabilizator vseh elementov (z izjemo enote) na množici vozlišč in na množici povezav prazen.

Zgled 3. *Oglejmo si delovanje $\mathbb{Z}$ na $Cay(\mathbb{Z}, \{1\})$ z (levim) seštevanjem. Poljuben element $n \in \mathbb{Z}$ porodi avtomorfizem $\rho_n(x) = n + x$. Grafično si to lahko predstavljamo kot translacijo cayleyevega grafa*



Hitro se prepričamo, da za vsak $n \in \mathbb{Z}$ *velja* $\rho_n(x) = n+x \neq x$ *za poljuben* $x \in V$ *in posledično tudi* $\{\rho_n(x), \rho_n(y)\} = \{x+n, y+n\} \neq \{x, y\}$ *za poljubne* $\{x, y\} \in E$*, torej je to primer prostega delovanja na grafu.*

Izkaže se, da ta zgled ni nobena partikularnost, za poljubno grupo namreč velja naslednji izrek.

Izrek 6. *Naj bo* G *grupa in* S *neka množica generatorjev* G*. Potem je delovanje* G *na* $Cay(G, S)$ *z levo translacijo*

$$g \cdot v = gv$$

prosto natanko tedaj, ko S *ne vsebuje nobenega elementa reda* 2*.*

Dokaz. Ker velja $g \cdot g' = gg'$ po definiciji delovanja in $gg' = g' \iff g = e$ zaradi dejstva da sta g in g' elementa grupe G, je delovanje G na vozliščih $Cay(G, S)$ vedno prosto, kar zadosti prvemu delu definicije za prosto delovanje na grafu. Dovolj je torej, da dokažemo ekvivalentnost drugega dela definicije.

Pokažimo, da v primeru, da delovanje ni prosto, $Cay(G, S)$ vsebuje element reda 2. Naj bo $g \in G$ in naj bo $\{v, v'\}$ povezava v $Cay(G, S)$ za katerega velja $\{v, v'\} = g \cdot \{v, v'\} = \{g \cdot v, g \cdot v'\}$ (druga enakost je definicija delovanja). Iz enakosti množic ločimo dva primera:

1. Lahko $g \cdot v = v$ in $g \cdot v' = v'$, kar pa je res le v primeru, da je $g = \varepsilon$, ker je delovanje na vozliščih prosto.

2. Če pa $g \cdot v = v'$ in $g \cdot v' = v$, po definiciji sosednosti v $Cay(G, S)$ obstaja $s \in (S \cup S^{-1}) \setminus \{\varepsilon\}$, da je $v' = vs$. Sledi:

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

   Če zdaj z leve množimo z v^{-1}, dobimo željeno enakost $e = s^2$. Torej je s iskani element reda 2.

Pokažimo še, da iz tega, da v S obstaja element reda 2, sledi, da delovanje ni prosto. Naj bo $s \in S$ reda 2. Pri delovanju G na $Cay(G, S)$ velja

$$s \cdot \{e, s\} = \{s \cdot e, s \cdot s\} = \{s, s^2\} = \{s, e\},$$

kar pomeni, da obstaja element grupe G ki fiksira neko povezavo, torej po definiciji dano delovanje na grafu ni prosto. □

S teorijo, ki smo jo do sem izpeljali, smo že skoraj pripravljeni podati opis prostih grup z njihovim delovanjem na drevesih. Od zaključka nas loči le že naslednji izrek.

Definicija 8 (Vpeto drevo delovanja)**.** *Naj grupa G deluje na povezanem graf X. **Vpeto drevo delovanja** G na X je podgraf grafa X, ki je drevo in vsebuje natanko eno vozlišče vsake orbite delovanja G na vozlišča grafa.*

Izrek 7. *Vsako delovanje grupe na povezanem grafu ima vpeto drevo delovanja.*

Dokaz. Naj bo G grupa, ki deluje na povezanem grafu X. Brez škode za splošnost je X neprazen, saj je drugače prazno drevo iskano vpeto drevo delovanja. Naj bo T_G družina poddreves X, ki vsebujejo največ en element vsake orbite delovanja G. Družina T_G je delno urejena za relacijo podgrafa, neprazna (vsebuje prazno drevo), vsaka veriga v T_G pa ima zgornjo mejo (konkretno unijo vseh elementov verige). Po Zornovi lemi sledi, da T_G vsebuje maksimalni element T. Ker je X neprazen je tudi T neprazen.

Zdaj pokažimo, da je T vpeto drevo delovanja. Denimo, da T ni vpeto drevo delovanja. Potemtakem obstaja neko vozlišče v, da nobeno od vozlišč v orbiti $G \cdot v$ ni vozlišče v T. S pomočjo vozlišča v bomo poiskali vozlišče v_0, za katerega bo veljalo, da nobeno od vozlišč v orbiti $G \cdot v_0$ ni v T, dodatno pa ima v_0 sosedno vozlišče, ki je v grafu T, iz česar bo sledilo protislovje.

Ker je X povezan obstaja pot p, ki povezuje neko vozlišče $u \in T$ z v. Naj bo v' prvo vozlišče v poti p, da $v' \notin T$. Ločimo dva primera:

1. Nobeno izmed vozlišč v $G \cdot v'$ ni v T. Potem je to iskano vozlišče $v_0 := v'$.

2. Obstaja $g \in G$, da $g \cdot v' \in T$. Označimo s p' pot med v' in v, ter z $g \cdot p'$ pot med $g \cdot v'$ in $g \cdot v$, kjer smo vsako vozlišče poti p' "premaknili" z delovanjem g. Ker je tako premaknjen $g \cdot v' \in T$, pot $g \cdot p'$ pa krajša od poti p, lahko postopek induktivno nadaljujemo, dokler ne najdemo želenega vozlišča (vozlišče zagotovo najdemo, ker za v noben element $G \cdot g \cdot v = G \cdot v$ ni v T).

Naj bo zdaj v vozlišče, za katerega noben element $G \cdot v$ ni v T in ima soseda $u \in T$. Če zdaj drevesu T dodamo vozlišče v in povezavo $\{u, v\}$ dobimo drevo v T_G, ki vsebuje T kot pravo poddrevo, kar je skregano s trditvijo zornove leme, da je T maksimalno. Torej je T vpeto drevo delovanja grupe G na povezanem grafu X. □

5 Delovanje prostih grup na drevesih

Pokažimo zdaj, da lahko proste grupe ekvivalentno opišemo z delovanjem na drevesih. Spodnji izrek nam poda geometrijski opis prostih grup, kot posledico, pa poda tudi zelo eleganten dokaz trditve, da so podgrupe proste grupe tudi same proste grupe, ki pa je žal izven obsega tega članka.

Če bralca zanima dokaz omenjene trditve in nadaljevanje teorije prostih grup naj se obrne na sekcijo 4.2.3 v članku [1].

Izrek 8. *Grupa je prosta natanko tedaj, ko ima neko prosto delovanje na nepraznem drevesu.*

Dokaz. ($\Longrightarrow$)

Naj bo F prosta grupa, prosto generirana z množico $S \subset F$. Po izreku 4 je njen Cayleyev graf $Cay(F, S)$ (neprazno) drevo. Po izreku 6 je delovanje F na $Cay(F, S)$ z levo translacijo prosto natanko tedaj, ko v S ni elementa reda 2. Uporabimo univerzalno lastnost prostih grup, da se prepričamo da S res nima elementov reda 2.

Naj bo $\varphi : S \longrightarrow \mathbb{Z}$ poljubna preslikava, za katero velja, da noben $s \in S$ ne slika v 0. Po univerzalni lastnosti jo lahko dopolnemo do homomorfizma $\overline{\varphi} : F \longrightarrow \mathbb{Z}$. Če $s \in S$ reda 2, mora red elementa $\overline{\varphi}(s)$ deliti 2. Red elementa $\overline{\varphi}(s)$ ne more biti 2, saj $(\mathbb{Z}, +)$ ne vsebuje elementov reda 2. Hkrati pa red elementa $\overline{\varphi}(s)$ ne more biti 1, ker je v $\mathbb{Z}$ edini element reda 1 element 0, ki pa po izbiri φ ni slika nobenega $s \in S$ (Spomnimo se, da $\overline{\varphi}|_S$ sovpada s φ). Na isti način bi lahko pokazali, da v prosti grupi noben element ne more imeti končnega reda.

Torej je delovanje proste grupe F na drevesu $Cay(F, S)$ z levo translacijo prosto.

($\Longleftarrow$)

Naj ima grupa G neko prosto delovanje na drevesu T. Po izreku 7 za to delovanje obstaja vpeto drevo delovanja.

Ideja dokaza je, da znotraj grafa T kontraktiramo T' in vsako njegovo translacijo $g \cdot T'$ (kjer $g \in G$) vsako v eno samo vozlišče. Na tako dobljeni graf bomo nato lahko gledali kot na graf $Cay(G, \widetilde{S})$, s čimer bomo dobili kandidata za množico S. Da S res prosto generira G, pa bo sledilo po izreku 5.

Preden začnemo s konstrukcijo kandidata poimenujmo z besedno zvezo **esencialne povezave** povezave v drevesu T, ki niso vsebovane v T', eno izmed vozlišč med katerima potekajo, pa je vsebovano v T' (drugo vozlišče zagotovo ne more biti vsebovano v T', saj bi drugače T vseboval cikel).

Začnimo zdaj s *konstrukcijo kandidata* $S \subset G$. Naj bo $e = \{u, v\}$ esencialna povezava T. Brez škode za splošnost je $u \in T'$ in $v \notin T'$. Ker je T'

vpeto drevo delovanja, obstaja $g_e \in G$, da $g_e^{-1} \cdot v \in T'$. Dodatno, ker orbita $G \cdot v$ vsebuje natanko en element v T' in ker G prosto deluje na T, sledi, da je g_e enolično določen.

Definirajmo

$$\widetilde{S} := \{g_e \in G \mid e \text{ je esencialna povezava } T\}.$$

Za množico $\widetilde{S}$ velja:

1. Po konstrukciji enota ni vsebovana v $\widetilde{S}$.

2. $\widetilde{S}$ ne vsebuje elementov reda 2.

   Če $g_e \in \widetilde{S}$ reda 2 za esencialno povezavo $e = \{u, v\}$ kot zgoraj, sledi $u_0 := g_e^{-1} \cdot v = g_e \cdot v \in T'$. Povezavo e slikamo v $g_e \cdot e = \{g_e \cdot u, u_0\}$

   (a) Če $u = u_0$, sledi $g_e \cdot e = e$, kar je protislovje s predpostavko o prostem delovanju.

   (b) Če $u \neq u_0$, sledi $\{u_0, g_e \cdot u\} \in g_e \cdot T = T$ (delovanje g_e je automorfizem). Znotraj T' obstaja pot med u_0 in u, znotraj $g_e \cdot T'$ (disjunkten s T') pa pot med $g_e \cdot u$ in v. Ker sta e in $g_e \cdot e$ povezavi T imamo v T cikel, kar je protislovje s tem, da je T drevo.

3. Če sta e in e' esencialni povezavi, za kateri sta $g_e = g_{e'}$, potem $e = e'$ (T je drevo, zato, kot zgoraj, ne moreta obstajati dve različni povezavi med povezanima T' in $g_e \cdot T' = g_{e'} \cdot T'$).

4. Če je $g \in \widetilde{S}$, denimo $g = g_e$ za neko esencialno povezavo e, potem je tudi $g^{-1} \cdot e$ esencialna povezava in $g^{-1} = g_{g^{-1} \cdot e} \in \widetilde{S}$.

   Z drugimi besedami, obstaja podmnožica $S \subset \widetilde{S}$, da velja:

$$S \cap S^{-1} = \emptyset \qquad \text{in} \qquad |S| = \frac{|\widetilde{S}|}{2} = \frac{1}{2} \cdot \#\text{ esencialnih povezav } T.$$

V naslednjem koraku pokažimo, da $\widetilde{S}$ (in posledično S) *generira* G. Naj bo $g \in G$ poljuben in $v \in T'$ poljubno vozlišče. Ker je T povezan, v njem med vozliščema v in $g \cdot v$ obstaja pot p. Pot p gre skozi več kopij T'. Označimo s $g_0 \cdot T', \ldots, g_n \cdot T'$ zaporedne kopije T', skozi katere vodi p, tako da velja $g_0 = e$, $g_n = g$ in $g_i \neq g_{i+1}$ za vsak $i \in \{0, \ldots, n-1\}$. Naj bo zdaj $j \in \{0, \ldots, n-1\}$ poljuben. Ker je T' vpeto drevo delovanja in je $g_i \neq g_{i+1}$, sta kopiji $g_j \cdot T'$ in $g_{j+1} \cdot T'$ povezani z neko povezavo e_j. Po definiciji je $g_j^{-1} \cdot e_j$ esencialna povezava, kateri smo v $\widetilde{S}$ priredili element

$$s_j := g_j^{-1} g_{j+1}$$

(bralec naj se sam prepriča da velja $s_j^{-1} \cdot v \in T'$, kjer $v \in g_j^{-1} \cdot e_j$, $v \notin T'$).

Vidimo, da velja

$$\begin{aligned} g = g_n &= g_0^{-1} g_n \\ &= g_0^{-1} g_1 g_1^{-1} g_2 \cdots g_{n-1}^{-1} g_n \\ &= s_0 s_1 \cdots s_{n-1} \end{aligned}$$

in g je element podgrupe generirane s $\widetilde{S}$. Ker je bil g poljuben sledi, da $\widetilde{S}$ generira G. Tako vidimo, da lahko, ko znotraj T kontraktiramo vse kopije T' vsako v eno samo vozlišče, novo dobljeni graf gledamo kot $Cay(G, \widetilde{S})$ (kopija $g \cdot T'$ po kontrakciji ustreza elementu g).

Ostane nam le še premislek, da $S \subset \widetilde{S}$, ki smo ga definirali zgoraj *prosto generira* G. Po izreku 5 zadošča dokazati, da $Cay(G, S)$ ne vsebuje ciklov (predpostavki $\forall s, t \in S : s \cdot t \neq e$ smo zadostili s 4. lastnostjo $\widetilde{S}$), kar pa bo držalo, ker lahko v primeru da imamo cikel, $Cay(G, S)$ razširimo nazaj v T, ter pridemo v protislovje s predpostavko, da je T drevo.

Naredimo torej to. Denimo, da obstaja $n \in \mathbb{N}$, $n \geq 3$ za katerega v $Cay(G, S) = Cay(G, \widetilde{S})$ obstaja cikel $g_0, \ldots, g_{n-1}$. Kot zgoraj so

$$\begin{aligned} s_{j+1} &:= g_j^{-1} g_{j+1} \quad j \in \{0, 1, \ldots, n-2\} \\ s_n &:= g_{n-1}^{-1} g_0 \end{aligned}$$

elementi $\widetilde{S}$. Naj bo e_i esencialna povezava med T' in $s_i \cdot T'$ za $i \in \{1, \ldots, n\}$. Oglejmo si povezavi e_i in e_{i+1} za $i \in \{1, \ldots, n-2\}$. Njuni translaciji $g_{i-1} \cdot e_i$ in $g_i \cdot e_{i+1}$ povezujeta translaciji $g_{i-1} \cdot T'$ z $g_i \cdot T'$ ter $g_i \cdot T'$ z $g_{i+1} \cdot T'$. Ker je $g_i \cdot T'$ drevo, znotraj njega obstaja pot med tistim vozliščem povezav $g_{i-1} \cdot e_i$ in $g_i \cdot e_{i+1}$, ki je v $g_i \cdot T'$. Vidimo torej, da obstaja pot med $g_0 \cdot T'$ in $g_{n-1} \cdot T'$. Ker pa $g_{n-1} \cdot e_n$ povezuje $g_{n-1} \cdot T'$ in $g_0 \cdot T'$ pomeni, da v T obstaja cikel, s čimer smo prišli v iskano protislovje.

□

Angleško-slovenski slovar strokovnih izrazov

free group prosta grupa
free generating set množica ki prosto generira
generating set množica generatorjev
universal property univerzalna lastnost
reduced word okrajšana beseda
cayley graph cayleyev graf
group action delovanje grupe
free action prosto delovanje
spanning tree vpeto drevo
spanning tree of an action vpeto drevo delovanja
essencial edge esencialna povezava

Literatura

[1] Löh Clara. *Geometric Group Theory: An Introduction (Universitext)*. Springer, kindle edition edition, 12 2017.