Proste grupe in drevesa
Seminar

Jakob Pogačnik Souvent
Fakulteta za matematiko in fiziko
Oddelek za matematiko

5. maj 2022

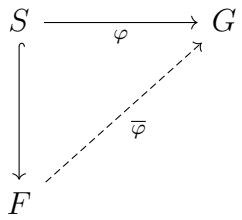
1 Uvod

TODO TODO: primeri

2 Proste grupe

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

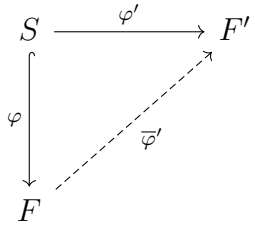
Za vsako grupo G in vsako preslikavo $\varphi : S \longrightarrow G$ obstaja enolično določen homomorfizem $\overline{\varphi} : F \longrightarrow G$ ki razširi φ.

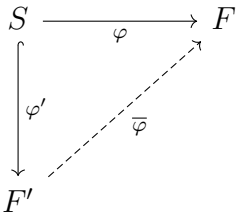


Grupi F pravimo ***prosta****, če vsebuje kakšno podmnožico, ki jo prosto generira, zgornji lastnosti pa pravimo* ***univerzalna lastnost*** *prostih grup.*

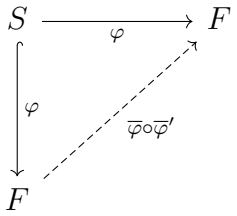
Izrek 1 (Enoličnost prostih grup)**.** *Naj bo S množica. Potem do izomorfizma natančno obstaja največ ena grupa prosto generirana z S.*

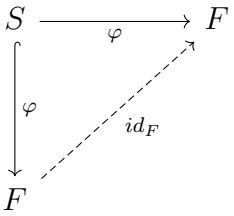
Dokaz. Naj bosta F in F' grupi, prosto generirani z S. Naj bosta $\varphi : S \hookrightarrow F$ in $\varphi' : S \hookrightarrow F'$ inkluziji. Po univerzalni lasnosti prostih grup lahko φ in φ' razširimo do homomorfizmov $\overline{\varphi}$ in $\overline{\varphi'}$.





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 obravnavamo φ kot 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 1. *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 S in njihovih inverzov, na katerih bomo uporabili le popolnoma očitno 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^* smatramo kot ekvivalentna, če se razlikujeta natanko za očitno uporabo pravila krajšanja (Opomba: popolnoma formalno je $\sim$ najmanjša ekvivalenčna relacija, 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

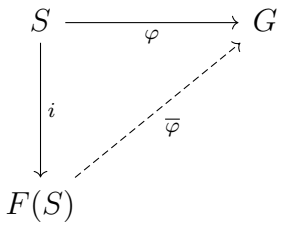
$$[x] \cdot [I(x)] = [I(I(x))] \cdot [I(x)] = [\varepsilon].$$

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 $i(S)$ generira $F(S)$.

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 $\varphi = \overline{\varphi} \circ i$. 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 generator 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 tudi F prosto generirana z S. □

Preden začnemo delati s prostimi grupami si poglejmo še alternativno konstrukcijo, ki nam bo pomagala pri razumevanju izrekov.

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*

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

   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.*

Dokaz. TODO □

Posledica 1. *Naj bo S množica. Vsak element proste grupe $F(S) = (S \cup \widehat{S})^* / \sim$ ustreza natanko eni okrajšani besedi nad $S \cup \widehat{S}$.*

Dokaz. Iz izreka 1 sledi $F(S) \cong F_{red}(S)$. □

3 Cayleyjevi grafi

Definicija 3 (Pot)**.** ***Pot*** *ki povezuje vozlišči v_0 in v_n v grafu $X = (V, E)$, je zaporedje 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 (Cayleyev graf)**.** *Naj bo S podmnožica, ki generira grupo G. **Cayleyjev graf** G glede na generator 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, ki generira G.

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

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 je protislovno, saj je v $F_{red}(S)$ to možno natanko tedaj, ko sta si s_i in s_{i+1} inverzna (inverz pa pomeni potovanje po isti povezavi v obratno smer). □

Opomba 2. *Inverz v splošnem ne drži. t.j. ni res da za vsak $Cay(F, S)$ sledi, da je F prosto generirana z S. TODO: protiprimer*

Izrek 5. *Naj bo G grupa in naj $S \subset G$ generira 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 $S \subset G$ 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 S generira G po predpostavki, avtomatično 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). Ločimo primere

1. Ker $\overline{\varphi}|_S = id_S$ mora biti $n > 1$.

2. Če $n = 2$ potem

$$e = \overline{\varphi}(s_1 s_2) = \overline{\varphi}(s_1)\overline{\varphi}(s_2) = s_1 s_2$$

   kar je v protislovju z našo predpostavko da $\forall s, t \in S : s \cdot t \neq e$.

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.

□

4 Delovanje

Definicija 5 (Delovanje)**.** *Naj bo G grupa, naj bo C kategorija in naj bo X objekt v C. **Delovanje** grupe G na X v kategoriji C je homomorfizem grup $G \longrightarrow Aut_C(X)$.*

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 $g, h \in G$.

Definicija 6 (Prosto delovanje na množici)**.** *Naj grupa G deluje na množici X. Pravimo, da je delovanje **prosto**, če velja:*

$$g \cdot x \neq x$$

za vsak $g \in G \setminus \{e\}$ in vsak $x \in X$.

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

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

Izrek 6. *Naj bo G grupa in S neka množica ki generira 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 in ustreza prvemu delu definicija 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. Če $g \cdot v = v$ in $g \cdot v' = v'$ kar pa je res le v primeru da $g = \varepsilon$, ker je delovanje na vozliščih prosto.

2. Če $g \cdot v = v'$ 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 desne 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

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

torej obstaja element grupe G ki fiksira neko povezavo in po definiciji dano delovanje na grafu ni prosto. □

Definicija 8 (Vpeto drevo delovanja)**.** *Naj grupa G deluje na povezan graf X.* ***Vpeto drevo delovanja*** *G na X je podgraf 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 iskano 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 z dejstvom, da je T maksimalno. Sledi, da je T iskano vpeto drevo delovanja grupe G na povezanem grafu. □

5 Delovanje prostih grup na drevesih

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 $S \subset F$ 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)

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. S tem 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 ni 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) $u = u_0 \Rightarrow g_e \cdot e = e$ protislovje s predpostavko o prostem delovanju.

(b) $u \neq u_0 \Rightarrow \{u_0, g_e \cdot u\} \in g_e \cdot T = T$ (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. Vidimo, da lahko, ko znotraj T kontraktiramo vse kopije T' vsako v eno samo vozlišče, novo dobljeni graf gledamo kot $Cay(G, \widetilde{S})$.

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

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

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.

□

6 Nielsen-Schreirerjev izrek