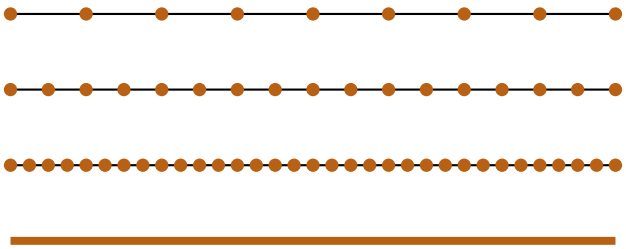
Teorija grup

Zapiski predavanj



Urban Jezernik

10. januar 2022

Kazalo

Kratek opis predmeta

Grupe so *osrednji objekt abstraktne algebre*. Njihova ključna lastnost je, da v njih lahko *množimo*, hkrati pa operacija množenja zadošča ravno dovolj aksiomom, da je mogoče o grupah povedati veliko s *strukturnega stališča*. Pri tem predmetu bomo govorili o različnih strukturnih aspektih grup, pri čemer nas bo vodila *rast*.

Za dano grupo $G = \langle S \rangle$, generirano z množico $S \subseteq G$, je njena *funkcija rasti* enaka

$$\texttt{rast}\colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto |\{s_1 s_2 \cdots s_n \mid s_i \in S \cup S^{-1} \cup \{1\}\}|,$$

in sicer izračuna število elementov grupe G, ki jih dobimo z množenjem največ n elementov množice S in njihovih inverzov.

Zgled.

- Naj bo $\mathbb{Z} = \langle 1 \rangle$. V tem primeru dobimo

  $$\texttt{rast}(n) = |\{-n, -n+1, \ldots, n\}| = 2n+1.$$

  Rast je torej linearna.

- Naj bo $\mathbb{Z}^2 = \langle (1,0), (0,1) \rangle$. V tem primeru dobimo

  $$\texttt{rast}(n) = |\{(x,y) \in \mathbb{Z}^2 \mid |x| + |y| \leq n\}| = 2n^2 + 2n + 1.$$

  Rast je torej kvadratna.

- Naj bo $F_2 = \langle x, y \rangle$ prosta grupa.[1] V tem primeru dobimo

  $$\begin{aligned} \texttt{rast}(n) &= \text{število besed v } x, y, x^{-1}, y^{-1} \text{ dolžine največ } n \\ &= 1 + 4 + 4 \cdot 3 + 4 \cdot 3 \cdot 3 + \cdots + 4 \cdot 3^{n-1} \\ &= 2 \cdot 3^n - 1. \end{aligned}$$

  Rast je torej eksponentna.

Pri predmetu bomo raziskovali *interakcijo* med asimptotskim obnašanjem rasti grup in njihovo algebraično strukturo. Podrobneje si bomo pogledali naslednje teme:

- *osnovni pojmi teorije grup*, končno prezentirane grupe;
- *delovanja*, Cayleyjev graf, prosta delovanja na drevesih;
- *struktura grup*, rešljive in nilpotentne grupe, razširitve;
- *rast*, tipi rasti, izračunljivost;
- *polinomska rast*, izrek Gromova;
- *srednja rast*, Grigorčukova grupa, amenabilnost;
- *eksponentna rast*, enakomernost, Breuillardova domneva.

[1] Vse osnovne definicije v zvezi z grupami bomo ponovili, tudi konstrukcijo proste grupe.

Literatura

Osnovne pojme teorije grup in geometrijska delovanja črpamo iz Löhine knjige, strukturo grup pa iz Mannove. Teorijo razširitev povzamemo iz Robinsonove monografije. Pri rasti se zopet naslonimo na Mannovo knjigo, s katero pokrijemo osnove in raziščemo grupe polinomske rasti. Pri dokazu izreka Gromova neenakost med topološko in Hausdorffovo dimenzijo pridobimo iz monografije Hurewicza in Wallmana. Obravnavo grup srednje rasti naslonimo na ekspozicijo Grugorčuka in Paka, povezavo z amenabilnostjo prikažemo kot v Mannovi knjigi, paradoksalne dekompozicije pa kot v Löhini. Pri grupah eksponentne rasti predstavimo zgled iz Osinovega članka in Bartholdijevo grupo, redukcijo hitro rastočih množic iz neskončnih v končne grupe pa prikažemo kot Breuillard, Green in Tao.

- C. Löh, *Geometric Group Theory – An Introduction*, Springer, 2017.
- A. Mann, *How Groups Grow*, London Mathematical Society Lecture Note Series 395, 2012.
- D. J. S. Robinson, *A Course in the Theory of Groups*, Springer, 1995.
- W. Hurewicz in H. Wallman, *Dimension Theory*, Princeton University Press, 1941.
- R. Grigorčuk in I. Pak, *Groups of intermediate growth: an introduction for beginners*, 2006.
- D. V. Osin, *The entropy of solvable groups*, Ergodic Theory Dynam. Systems 23 (2003), 907–918.
- L. Bartholdi, *A Wilson group of non-uniformly exponential growth*, Comptes Rendus Mathematique 336.7 (2003), 549–554.
- E. Breuillard, B. Green, T. Tao, *The structure of approximate groups*, Publications mathématiques de l'IHÉS 116 (2012), 115-–221.

Poglavje 1

Osnovni pojmi

1.1 Kategorija grup

Abstraktne grupe

Grupa je množica G z binarno operacijo $\cdot : G \times G \to G$, ki zadošča aksiomom:

- asociativnost: $\forall g_1, g_2, g_3 \in G : (g_1 g_2) g_3 = g_1 (g_2 g_3)$;
- obstoj enote: $\exists 1 \in G \ \forall g \in G : 1g = g1 = g$;
- obstoj inverzov: $\forall g \in G \ \exists g^{-1} \in G : gg^{-1} = g^{-1}g = 1$.

Množica $H \subseteq G$ je podgrupa, če je grupa glede na zožitev $\cdot|_{H \times H}$. V tem primeru dobimo množico odsekov $G/H = \{gH \mid g \in G\}$, kjer je $gH = \{g \cdot h \mid h \in H\}$. Kardinalnost množice odsekov je indeks $|G : H|$.

Za dani grupi G, H je preslikava $\varphi : G \to H$ homomorfizem, če velja $\forall g_1, g_2 \in G : \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$. Bijektivni homomorfizem je izomorfizem, v tem primeru pišemo $G \cong H$. Jedro je $\ker \varphi = \{g \in G \mid \varphi(g) = 1\}$, slika je $\operatorname{im} \varphi = \{\varphi(g) \mid g \in G\}$.

Konkretne grupe

Zgornja aksiomatizacija koncepta grupe izhaja iz konkretnih modelov simetrij geometrijskih ali algebraičnih objektov.

Zgled. Naj bo X množica. *Simetrična grupa* je $\operatorname{Sym}(X) = \{f : X \to X \mid f \text{ bijekcija}\}$. Za $X = \{1, 2, \ldots, n\}$ dobimo $\operatorname{Sym}(X) = S_n$.

Vsaka abstraktna grupa izhaja iz simetrične grupe.

Trditev. (CAYLEYJEV IZREK) Vsaka grupa je izomorfna podgrupi neke simetrične grupe.

Dokaz. G je izomorfna podgrupi $\operatorname{Sym}(G)$:

$$f : G \to \operatorname{Sym}(G), \quad f(g) : x \mapsto g \cdot x \quad (x \in G).$$

Preslikava f je injektiven homomorfizem. □

Nasploh imajo množice preslikav, ki ohranjajo neko strukturo, ponavadi strukturo grupe. V naravi se grupe pojavljajo v taki obliki.

Zgled.

- Naj bo G grupa. Priredimo ji njeno *grupo avtomorfizmov* $\mathrm{Aut}(G) = \{f : G \to G \mid f \text{ izomorfizem}\}$.
- Naj bo X metrični prostor. Priredimo mu *grupo izometrij*[1] $\mathrm{Isom}(X) = \{f : X \to X \mid f \text{ izometrija}\}$.
- Naj bo V vektorski prostor nad poljem k. Priredimo mu *matrično grupo* $\mathrm{Aut}(V) = \{f : V \to V \mid f \text{ linearen izomorfizem}\} = \mathrm{GL}(V)$.
- Naj bo L/K Galoisjeva razširitev polj. Priredimo ji *Galoisjevo grupo* $\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}_K\}$.

Obstajajo pa tudi druge pojavitve grup v matematiki.

Zgled. Topološkemu prostoru X priredimo *fundamentalno grupo* $\pi_1(X)$ in *homološke grupe* $H_i(X)$.

Edinke in kvocienti

Naj bo G grupa. Podgrupa $N \leq G$ je edinka, če je invariantna za konjugiranje:

$$\forall n \in N \ \forall g \in G : gng^{-1} \in N.$$

Pišemo $N \trianglelefteq G$. V tem primeru ima množica odsekov G/N strukturo grupe: $g_1N \cdot g_2N = g_1g_2N$. To je kvocientna grupa. Kvocientna projekcija je homomorfizem

$$\pi : G \to G/N, \quad g \mapsto gN \qquad (g \in G).$$

Zgled. Grupa celih števil $\mathbb{Z}$ za seštevanje je edinka v grupi realnih števil $\mathbb{R}$ za seštevanje. Kvocientna grupa je $\mathbb{R}/\mathbb{Z} \cong S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, izomorfizem podaja preslikava $r + \mathbb{Z} \mapsto e^{2\pi i r}$.

1.2 Generatorji in relacije

Kadar želimo najti kakšno grupo *s posebnimi algebraičnimi lastnostmi*, je včasih težko najti objekt, ki nam bo prek avtomorfizmov dal želeno grupo. V tem primeru velikokrat uporabimo abstraktno konstrukcijo grupe z *generatorji in relacijami*.

Generatorji grup

Naj bo G grupa in $S \subseteq G$ njena podmnožica. Podgrupa, generirana s S, je najmanjša podgrupa grupe G, ki vsebuje S. Oznaka: $\langle S \rangle$. Velja

$$\langle S \rangle = \{s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \mid n \in \mathbb{N},\ s_i \in S,\ \epsilon_i \in \{1, -1\}\}.$$

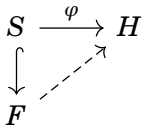
Rečemo, da S generira G, če velja $\langle S \rangle = G$. Če G vsebuje kakšno *končno* podmnožico S, ki generira G, je G končno generirana grupa.

Zgled. $\mathbb{Z} = \langle 1 \rangle = \langle 2, 3 \rangle > \langle 2 \rangle = 2 \cdot \mathbb{Z}$.

[1] Izometrija $f : X \to X$ je bijektivna preslikava, za katero velja $\forall x, y \in X : d(x, y) = d(f(x), f(y))$.

Proste grupe

Grupa F je prosto generirana s $S \subseteq F$, če ima naslednjo *univerzalno lastnost*: za vsako grupo H in vsako preslikavo $\varphi: S \to H$ obstaja natanko en homomorfizem $\bar{\varphi}: F \to H$, ki razširja φ, to je $\bar{\varphi}(s) = \varphi(s)$ za vsak $s \in S$.



Grupa je prosta, če je prosto generirana s kakšno podmnožico.

Zgled.

- $\mathbb{Z}$ je prosto generirana z $\{1\}$, ne pa z $\{2,3\}$.
- $\mathbb{Z}/2\mathbb{Z}$ *ni* prosta.

Iz vsake množice S lahko prosto generiramo grupo na naslednji način.

Izrek. Naj bo S množica. Tedaj obstaja grupa, prosto generirana z S. Ta grupa je enolična do izomorfizma natančno.

Dokaz. Dokažimo le obstoj, enoličnost sledi iz univerzalne lastnosti prosto generiranih grup.

Vpeljimo abecedo $A = S \cup \hat{S}$, kjer je $\hat{S} = \{\hat{s} \mid s \in S\}$ disjunktna kopija množice S (njeni elementi igrajo vlogo s^{-1} za $s \in S$).

Naj bo A^* množica vseh zaporedij (*besed*) simbolov iz A. Ta vsebuje prazno besedo, ki jo označimo z ϵ. Besede lahko množimo s konkatenacijo: $x \cdot y = xy$ za $x, y \in A^*$.

Uvedimo ekvivalenčno relacijo $\sim$ na A^* (*krajšanje*): za vse $x, y \in A^*$ in $s \in S$ zahtevajmo $xs\hat{s}y \sim xy$ in $x\hat{s}sy \sim xy$.

Naj bo $F(S) = A^*/\sim$. Konkatenacija inducira množenje na $F(S)$: $[x] \cdot [y] = [xy]$.

$F(S)$ je grupa: Enota je $[\epsilon]$, inverze izračunamo induktivno z $[s \cdot x]^{-1} = [x]^{-1} \cdot [\hat{s}]$ in $[\hat{s} \cdot x]^{-1} = [x]^{-1} \cdot [s]$ za $s \in S, x \in A^*$. ✓✓

$F(S)$ je prosto generirana s S: Imamo naravno preslikavo $S \to F(S), s \mapsto [s]$. Naj bo $\varphi: S \to G$ neka preslikava za neko grupo G. Potem φ lahko razširimo do homomorfizma $\bar{\varphi}: F(S) \to G$ induktivno: $\bar{\varphi}([s \cdot x]) = \varphi(s) \cdot \bar{\varphi}([x])$, $\bar{\varphi}([\hat{s} \cdot x]) = \varphi(s)^{-1} \cdot \bar{\varphi}([x])$ za $s \in S, x \in A^*$. ✓✓ □

Elementi grupe $F(S)$ so torej *okrajšane besede* s črkami iz $S \cup S^{-1}$, množimo pa jih s konkatenacijo. Tukaj uporabljamo oznako $S^{-1} = \{s^{-1} \mid s \in S\}$.

Prosta grupa ranga n je $F_n = F(\{1, \ldots, n\})$. Enolična je do izomorfizma natančno.

Grupa je končno generirana, če in samo če je kvocient proste grupe ranga n za nek n (sledi iz univerzalne lastnosti).

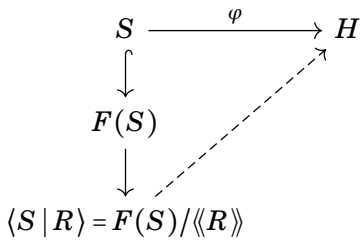
Generatorji in relacije

Naj bo G grupa in $S \subseteq G$. Edinka, generirana s S, je najmanjša edinka v G, ki vsebuje S. Oznaka: $\langle\langle S \rangle\rangle$. Velja:

$$\langle\langle S \rangle\rangle = \left\{ g_1 s_1^{\epsilon_1} g_1^{-1} g_2 s_2^{\epsilon_2} g_2^{-1} \cdots g_n s_n^{\epsilon_n} g_n^{-1} \mid n \in \mathbb{N},\ g_i \in G,\ s_i \in S,\ \epsilon_i \in \{1, -1\} \right\}.$$

Naj bo $F(S)$ prosto generirana s S. Naj bo $R \subseteq F(S)$ neka podmnožica. Naj bo $\langle S \mid R \rangle = F(S)/\langle\langle R \rangle\rangle$, to je grupa, generirana s S z relacijami R. Če za neko grupo G velja $G \cong \langle S \mid R \rangle$, je par (S,R) prezentacija grupe G z generatorji S in relacijami R.

Grupa $\langle S \mid R \rangle$ ima naslednjo *univerzalno lastnost*: za vsako grupo H in vsako preslikavo $\varphi: S \to H$, katere enolična razširitev $\varphi^*: (S \cup S^{-1})^* \to H$ zadošča $\varphi^*(r) = 1$ za vsak $r \in R$, obstaja natanko en homomorfizem $\bar{\varphi}: \langle S \mid R \to H$, ki razširja φ, to je $\bar{\varphi}(s) = \varphi(s)$ za vsak $s \in S$.



Ta lastnost sledi neposredno iz univerzalne lastnosti proste grupe in univerzalne lastnosti kvocientne projekcije $\pi: F(S) \to \langle S \mid R \rangle$.

Zgled.

- $\mathbb{Z}/n\mathbb{Z} \cong \langle x \mid x^n \rangle$. Izomorfizem izhaja iz $F(\{x\}) \cong \mathbb{Z}$, $\langle\langle \{x^n\} \rangle\rangle \cong \langle n \rangle \leq \mathbb{Z}$.

- Naj bo X_n pravilni n-kotnik v ravnini. Grupo izometrij $Isom(X_n)$ imenujemo diedrska grupa in označimo z D_{2n}. Trdimo, da velja:

  $$D_{2n} \cong \langle s,t \mid s^n, t^2, tst^{-1} = s^{-1} \rangle.$$

  Tukaj zlorabljamo oznako, $S = \{s,t\}$, $R = \{s^n, t^2, tst^{-1} \cdot s\}$.

  Označimo $G = \langle S \mid R \rangle$. Naj bo $\sigma \in D_{2n}$ rotacija za kot $2\pi/n$ okoli središča X_n, in naj bo $\tau \in D_{2n}$ zrcaljenje X_n preko enega vozlišča. Velja $\sigma^n = \tau^2 = 1$ in $\tau\sigma\tau^{-1} = \sigma^{-1}$. Iz univerzalne lastnosti G dobimo homomorfizem $\bar{\varphi}: G \to D_{2n}$, ki slika $s \mapsto \sigma, t \mapsto \tau$.

  Velja $D_{2n} = \{\sigma^i \mid 0 \leq i \leq n-1\} \cup \{\tau\sigma^i \mid 0 \leq i \leq n-1\}$, torej je $|D_{2n}| = 2n$.

  Definirajmo preslikavo $\psi: D_{2n} \to G$, ki preslika $\sigma^i \mapsto s^i, \tau\sigma^i \mapsto ts^i$. Preprost račun pokaže, da je ψ homomorfizem, ki je inverzen $\bar{\varphi}$. Res torej velja $D_{2n} \cong G$.

- Kateri znani grupi je izomorfna grupa

  $$G = \langle x,y \mid xyx^{-1} = y^2,\ yxy^{-1} = x^2 \rangle?$$

  V grupi G velja račun: $xyx^{-1} = y^2$, zato $x \cdot xyx^{-1} = xy^2$, od koder sledi $yxy^{-1} \cdot yx^{-1} = xy^2$, to pa implicira $y = xy^2$, zato je nujno $x = y^{-1}$. Iz prve relacije v definiciji G zdaj sledi $y = 1$, s tem pa tudi $x = 1$. Ker $\{x,y\}$ generira G, sklepamo $G \cong 1$, torej je G trivialna grupa.

Ali lahko iz prezentacije ugotovimo (na primer z računalniškim programom) ali je dana grupa trivialna? V splošnem je odgovor *ne*! Besedni problem za grupo $\langle S \mid R \rangle$ sprašuje, če se lahko ob vnosu besede $x \in (S \cup S^{-1})^*$ odločimo (z algoritmom), ali je $x = 1$ v $\langle S \mid R \rangle$.[2] Ta problem je za nekatere grupe preprosto rešljiv, na primer za grupo $\langle 1 \mid \varnothing \rangle \cong \mathbb{Z}$. Obstajajo pa

[2] Tu imamo v resnici dve vprašanji. 1. Ali obstaja algoritem, ki se ob vnosu x ustavi, če je le $x = 1$ v grupi? 2. Ali obstaja algoritem, ki se ob vnosu x ustavi, če je le $x \neq 1$ v grupi? Kasneje bomo videli, da je odgovor na prvo vprašanje vedno pritrdilen, težave pa so z drugim vprašanjem.

grupe $\langle S \mid R \rangle$ (celo z $|S|, |R| < \infty$), za katere je besedni problem neodločljiv (Novikov 1955) – takega algoritma ni![3]

Končno prezentirane grupe

Grupa G je končno prezentirana, če ima kakšno prezentacijo $G \cong \langle S \mid R \rangle$ z $|R|, |S| < \infty$.

Končno prezentirane grupe so vedno končno generirane, obratno pa v splošnem ne drži.

Zgled. Naj bo $L = \langle a, t \mid a^2, [t^k a t^{-k}, t^j a t^{-j}] \text{ za vse } j,k \in \mathbb{Z} \rangle$.[4] Grupa L se imenuje svetilkarjeva grupa.[5]

Grupa L *ni* končno prezentirana (→ vaje).

Grupo L lahko uresničimo na bolj konkreten način kot podgrupo matrik preko homomorfizma

$$\varphi : L \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}[x, x^{-1}])$$

iz L v matrike nad kolobarjem Laurentovih polinomov[6] nad $\mathbb{Z}/2\mathbb{Z}$, ki preslika generatorja na naslednji način:

$$\varphi : a \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad t \mapsto \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}.$$

S to definicijo velja $\varphi(a^2) = 1$ in $\varphi([t^k a t^{-k}, t^l a t^{-l}]) = 1$, zato po univerzalni lastnosti res dobimo homomorfizem φ.

Lahko je preveriti, da velja

$$\operatorname{im} \varphi = \left\{ \begin{pmatrix} x^k & P \\ 0 & 1 \end{pmatrix} \mid k \in \mathbb{Z},\ P \in \mathbb{Z}/2\mathbb{Z}[x, x^{-1}] \right\}.$$

Z nekaj truda se da napisati tudi inverzno preslikavo $\psi : \operatorname{im} \varphi \to L$ (→ vaje). Zato velja $L \cong \operatorname{im} \varphi$, s čimer smo abstraktno grupo L uresničili kot podgrupo matrik.

1.3 Nove grupe iz starih

Pogledali si bomo nekaj standardnih konstrukcij novih grup iz starih.

Produkti

Naj bo I indeksna množica in $(G_i)_{i \in I}$ družina grup. Tvorimo njihov direktni produkt $\prod_{i \in I} G_i$: to je množica $\prod_{i \in I} G_i$, opremljena z operacijo po komponentah, se pravi $(g_i)_{i \in I} \cdot (h_i)_{i \in I} = (g_i h_i)_{i \in I}$. Direktna vsota $\bigoplus_{i \in I} G_i$ je podgrupa direktnega produkta, ki sestoji iz elementov $(g_i)_{i \in I}$, za katere velja $g_i = 1$ za vse razen končno mnogo komponent.

[3] Turingov stroj lahko zakodiramo v grupo, pravila zakodiramo v relacije, črke in stanja zakodiramo v generatorje.

[4] Oznaka $[x, y]$ stoji za komutator $x^{-1} y^{-1} x y$.

[5] Angleško *lamplighter group*.

[6] Element tega kolobarja je na primer $x^{-2} + 1 + x^{10}$.

Razširitve

Grupe lahko združimo tudi na bolj zakomplicirane načine. Za dani grupi N, Q je razširitev Q z N eksaktno zaporedje grup

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1,$$

torej $\ker \iota = 1$, $\operatorname{im} \pi = Q$, $\operatorname{im} \iota = \ker \pi$.

Zgled.

- $0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$, kjer je $\iota(x) = (x, 0)$ in $\pi(x, y) = y$.

  V tem primeru imamo trivialno razširitev, kjer je srednja grupa G kar direktni produkt grup Q in N.

- $0 \to \mathbb{Z} \xrightarrow{\iota} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0$, kjer je $\iota(n) = 2n$ in $\pi(n) = n \mod 2$.

  Srednja grupa v razširitvi v tem primeru *ni* kar direktni produkt grup Q in N.

Semidirektni produkti

Obstajajo razširitve, ki so le malo deformirani direktni produkti. Za dani grupi Q, N in dan homomorfizem[7] $\varphi : Q \to \operatorname{Aut}(N)$ je semidirektni produkt Q z N glede na φ grupa $N \rtimes_\varphi Q$, ki je kot množica $N \times Q$, operacija pa je definirana kot $(n_1, q_1) \cdot (n_2, q_2) = (n_1 \varphi(q_1)(n_2), q_1 q_2)$. V primeru, ko za vsak $q \in Q$ velja $\varphi(q) = \mathrm{id}_N$, dobimo $N \rtimes_\varphi Q = N \times Q$, torej kar običajen direktni produkt grup.

Zgled.

- Vemo že, da lahko diedrsko grupo predstavimo kot $D_{2n} = \langle s, t \mid s^n, t^2, tst^{-1} = s^{-1} \rangle$. Zdaj jo bomo predstavili še kot semidirektni produkt.

  Naj bo $\varphi : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})$, $1 \mapsto (x \mapsto -x)$. Tvorimo $G = \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$. Preslikava $f : D_{2n} \to G$, dana s predpisom $s \mapsto (1, 0), t \mapsto (0, 1)$, je homomorfizem. Velja $\operatorname{im} f = G$ in $|D_{2n}| = |G| = 2n$, zato je f izomorfizem.

  Podobno velja v limiti $n \to \infty$. Naj bo $D_\infty = \langle s, t \mid t^2, tst^{-1} = s^{-1} \rangle$. Naj bo $\varphi : \mathbb{Z}/2\mathbb{Z} \to \operatorname{Aut}(\mathbb{Z})$, $1 \mapsto (x \mapsto -x)$. Tedaj imamo izomorfizem $D_\infty \cong \mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, ki izhaja iz prirejanja $s \mapsto (1, 0), t \mapsto (0, 1)$.

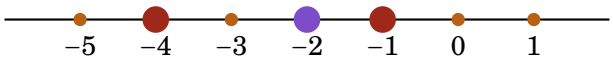
- Spomnimo se svetilkarjeve grupe

  $$L = \left\langle a, t \mid a^2, [t^k a t^{-k}, t^j a t^{-j}] \text{ za vse } j, k \in \mathbb{Z} \right\rangle.$$

  Element $a \in L$ je reda 2, torej imamo eno kopijo $\mathbb{Z}/2\mathbb{Z}$ v L. Element $t \in L$ je neskončnega reda, kar nam da eno kopijo $\mathbb{Z}$ v L. Element t^k konjugira a v $t^k a t^{-k}$. Za vsak $k \in \mathbb{Z}$ dobimo torej eno kopijo $\mathbb{Z}/2\mathbb{Z}$ v L. Vse te različne kopije med sabo komutirajo, torej v L najdemo $\bigoplus_{i \in \mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.

  Definirajmo $\varphi : \mathbb{Z} \to \bigoplus_{i \in \mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, $i \mapsto ((g_n)_{n \in \mathbb{Z}} \mapsto (g_{n+i})_{n \in \mathbb{Z}})$. Tvorimo grupo $\left(\bigoplus_{i \in \mathbb{Z}} \mathbb{Z}/2\mathbb{Z}\right) \rtimes_\varphi \mathbb{Z}$. Trdimo, da je ta semidirektni produkt

[7] Torej Q deluje na N. O delovanjih bomo podrobneje govorili v naslednjem poglavju.



Slika 1.1: Svetlikar se sprehaja in prižiga svetilke

izomorfen grupi L. Generatorjema a in t bosta pri tem ustrezala elementa $A = (e_0, 0)$ in $T = (0, 1)$, kjer smo z $e_i \in \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ označili bazni vektor, ki je pri i-ti komponenti enak 1, sicer pa 0.

Definirajmo najprej preslikavo $\alpha: L \to (\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathbb{Z}$, $a \mapsto A, t \mapsto T$. S tem res dobimo induciran homomorfizem grup po univerzalni lastnosti, saj se relatorji L preslikajo v enoto. Velja namreč $A^2 = (2e_0, 0) = (0, 0)$, $TAT^{-1} = (0, 1)(e_0, 0)(0, -1) = (e_{-1}, 0)$, $T^k A T^{-k} = (e_{-k}, 0)$ in zatorej $[T^k A T^{-k}, T^j A T^{-j}] = (0, 0)$.

Definirajmo zdaj še inverzni homomorfizem $\beta: (\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathbb{Z} \to L$. Ta naj po definiciji slika $(e_0, n) \mapsto a t^n$, $(e_{-k}, 0) \mapsto t^k a t^{-k}$. Od tod izpeljemo kandidata za splošno formulo za β: $(\sum_{k\in\mathbb{Z}} a_{-k} e_{-k}, n) \mapsto \prod_{k\in\mathbb{Z}} (t^k a t^{-k})^{a_{-k}} \cdot t^n$. Ker so skoraj vsi koeficienti a_k enaki 0, je zadnji produkt končen. Lahko je preveriti (→ vaje), da je β res homomorfizem, ki je inverzen α.

Torej je res $(\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}) \rtimes_\varphi \mathbb{Z} \cong L$.

Zdaj lahko pojasnemo ime svetilkarjeva grupa. Element L je prek izomorfizma zgoraj določen z elementom iz $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ (= končno mnogo izbir 1 iz množice $\mathbb{Z}$) in z elementom iz $\mathbb{Z}$.

Predstavljajmo si, imamo za vsak element iz $\mathbb{Z}$ svetilko, ki je bodisi prižgana bodisi ugasnjena. Svetilkar je na začetku službe na poziciji $0 \in \mathbb{Z}$. Prvi element pri izbiri elementa v L nam pove, katere svetilke je svetilkar prižgal. Drugi element nam pove, kje je svetilkar na koncu službe.

Element grupe L je beseda v a in t, na primer tat^3at^{-2}. To s svetilkarjem interpretiramo takole: svetilkar začne v $0 \in \mathbb{Z}$, potem se premakne za 1 v levo, prižge svetilko, se premakne za 3 v levo, prižge svetilko, se premakne za 2 v desno in se ustavi. Na koncu sta svetilki prižgani na pozicijah $-1, -4$, svetilkar sam pa je na poziciji -2. To ustreza naslednjemu računu v L:

$$tat^3at^{-2} = tat^{-1} \cdot t^4 a t^{-4} \cdot t^2 \equiv (e_{-1} + e_{-4}, 2).$$

Semidirektni produkti se pojavijo v posebnih vrstah razširitev. Razcepna razširitev je razširitev $1 \to N \to G \xrightarrow{\pi} Q \to 1$, v kateri obstaja *homomorfizem* $s: Q \to G$, ki zadošča $\pi \circ s = \mathrm{id}_Q$. Takemu homomorfizmu rečemo prerezni homomorfizem.

Za dani grupi N, Q in delovanje $\varphi: Q \to \mathrm{Aut}(N)$ imamo razcepno razširitev

$$1 \to N \to N \rtimes_\varphi Q \to Q \to 1$$

z vložitvijo $n \mapsto (n, 1)$, projekcijo $(n, q) \mapsto q$ in prereznim homomorfizmom $q \mapsto (1, q)$.

Velja tudi obratno. Naj bo $1 \to N \to G \to Q \to 1$ razcepna razširitev s prereznim homomorfizmom s. Tedaj dobimo delovanje Q na N: $\varphi: Q \to \mathrm{Aut}(N)$, $q \mapsto (n \mapsto s(q) \cdot n \cdot s(q)^{-1})$. Element q torej s s dvignemo v G in konjugiramo element n. Pri tem velja $G \cong N \rtimes_\varphi Q$, izomorfizem izhaja iz $(n, q) \mapsto n \cdot s(q)$ in $g \mapsto (g \cdot (s \circ \pi(g))^{-1}, \pi(g))$.

S tem smo premislili vsebino naslednje trditve.

Trditev. Semidirektni produkti so natanko grupe, ki se pojavijo kot razširitve v razcepnih razširitvah.

Več o razširitvah si bomo pogledali nekoliko kasneje.

Poglavje 2

Delovanja

Bistvo grup je, da delujejo – na različnih objektih.

2.1 Delovanja grup

Osnovno o delovanjih

Bodi G grupa, $\mathcal{C}$ kategorija in X objekt v $\mathcal{C}$. Delovanje grupe G na X je homomorfizem $G \xrightarrow{\rho} \mathrm{Aut}_{\mathcal{C}}(X)$.

Zgled.

- Za $\mathcal{C}$ vzemimo kategorijo množic. Naj bo X množica. Delovanje G na X je homomorfizem $G \xrightarrow{\rho} \mathrm{Sym}(X)$ iz G v grupo bijekcij množice X.
- Za $\mathcal{C}$ vzemimo kategorijo topoloških prostorov. Naj bo X topološki prostor. Delovanje G na X je homomorfizem $G \xrightarrow{\rho} \mathrm{Homeo}(X)$ iz G v grupo homeomorfizmom prostora X.
- Za $\mathcal{C}$ vzemimo kategorijo vektorskih prostorov. Naj bo V vektorski prostor. Delovanje G na V je homomorfizem $G \xrightarrow{\rho} \mathrm{GL}(V)$ iz G v grupo linearnih avtomorfizmov prostora V. Ta zadnji primer je še posebej pomemben, saj grupo G uresničimo kot grupo linearnih transformacij vektorskega prostora. V tem primeru rečemo, da je ρ upodobitev grupe G.

Cayleyjevo delovanje

Cayleyjevo delovanje je najpomembnejši primer delovanja. Izhaja iz Cayleyjevega izreka:

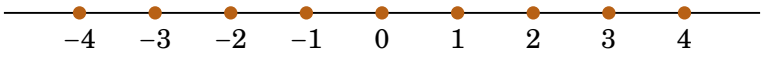
$$G \to \mathrm{Sym}(G), \quad g \mapsto (x \mapsto g \cdot x) \quad (g, x \in G).$$

To delovanje grupe G na množici G si lahko vizualiziramo z grafom na naslednji način.

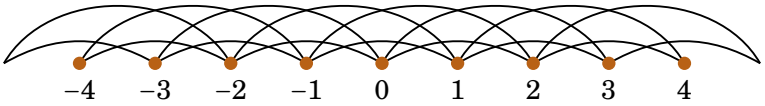
Dana je grupa G in $S \subseteq G$ neka njena generirajoča podmnožica. Cayleyjev graf grupe G glede na S je graf $\mathrm{Cay}(G, S)$ z:

- vozlišči $V = G$,[1]
- povezavami $E = \{\{g, g \cdot s\} \mid g \in G,\ s \in S \cup S^{-1} \setminus \{1\}\}$.

[1] Za vsak element $g \in G$ imamo torej eno vozlišče.



Slika 2.1: $\mathrm{Cay}(\mathbb{Z},\{1\})$



Slika 2.2: $\mathrm{Cay}(\mathbb{Z},\{2,3\})$

Zgled.

- $\mathrm{Cay}(\mathbb{Z},\{1\})$ je pot neskončne dolžine.
- $\mathrm{Cay}(\mathbb{Z},\{2,3\})$ je 4-regularen graf, ki pa ni drevo.
- $\mathrm{Cay}(\mathbb{Z}^2,\{(1,0),(0,1)\})$ je ravninska mreža.
- $\mathrm{Cay}(\mathbb{Z}/6\mathbb{Z},\{1\})$ je 6-cikel.
- $\mathrm{Cay}(S_3,\{\tau,\sigma\})$, kjer je $\tau = (1\ 2)$ in $\sigma = (1\ 2\ 3)$, je tristrana prizma z eno *križno* povezavo.
- $\mathrm{Cay}(F_2,\{x,y\})$ je 4-regularno drevo.

Proste grupe so natanko grupe, katerih Cayleyjev graf je *lahko* drevo.[2]

Trditev. Naj bo G grupa in $S \subseteq G$ z lastnostjo $S \cap S^{-1} = \varnothing$. Če je $\mathrm{Cay}(G,S)$ drevo, potem S prosto generira G.

Dokaz. Po univerzalni lastnosti proste grupe dobimo homomorfizem $\varphi: F(S) \to G$. Ker S generira G, je φ surjektiven. Privzemimo, da φ *ni* injektiven. Naj bo $1 \neq w = s_1 \cdots s_n \in F(S)$ $(s_i \in S \cup S^{-1})$ okrajšana beseda minimalne dolžine, ki je v jedru $\ker\varphi$. Ločimo več primerov glede na dolžino besede.

- *Če je* $n = 1$*:* V tem primeru je $w = s_1 \in S \cup S^{-1}$. Toda $\varphi|_S$ je injektivna. Protislovje s predpostavko $\varphi(w) = 1$.

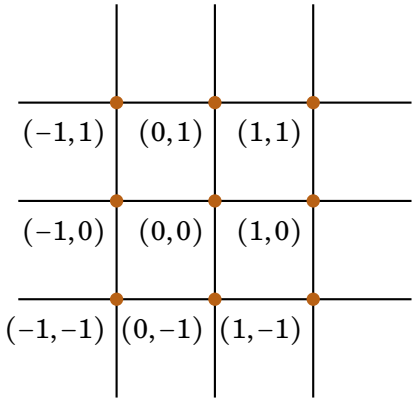
- *Če je* $n = 2$*:* V tem primeru je $w = s_1 s_2$ in velja $\varphi(w) = 1$. Torej $1 = \varphi(s_1 s_2) = s_1 \cdot s_2 \in G$. Torej je $s_1 \neq s_2^{-1}$ v $F(S)$,[3] medtem ko je $s_1 = s_2^{-1}$ v G. Od tod sledi $s_1 \in S \cap S^{-1} \subseteq G$. Protislovje s predpostavko $S \cap S^{-1} = \varnothing$.

- *Če je* $n \geq 3$*:* Zaporedje elementov $1, s_1, s_1 s_2, \ldots, s_1 s_2 \cdots s_n$ tvori cikel v $\mathrm{Cay}(G,S)$, saj je $s_1 s_2 \cdots s_n = \varphi(w) = 1 \in G$. Vsa vozlišča tega cikla so *različna* med sabo: če je namreč $s_1 \cdots s_i = s_1 \cdots s_j \in G$ za nek $i < j$, potem je beseda $w' = s_1 s_2 \cdots s_i s_{j+1} \cdots s_n \in F(S)$ krajše dolžine kot w, hkrati pa velja $\varphi(w') = s_1 s_2 \cdots s_i s_{j+1} \cdots s_n = s_1 s_2 \cdots s_j s_{j+1} \cdots s_n = \varphi(w) = 1$. Protislovje z minimalnostjo dolžine $w \in \ker\varphi$. Tako res dobimo n-cikel v grafu $\mathrm{Cay}(G,S)$. Protislovje s predpostavko, da je $\mathrm{Cay}(G,S)$ drevo.

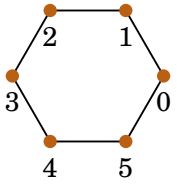
□

[2] Trditev nam podaja *geometrijsko* karakterizacijo prostih grup. V naslednjem razdelku jo bomo še razširili.

[3] Beseda w je okrajšana.



Slika 2.3: $\mathrm{Cay}(\mathbb{Z}^2, \{(1,0),(0,1)\})$



Slika 2.4: $\mathrm{Cay}(\mathbb{Z}/6\mathbb{Z}, \{1\})$

Prosta delovanja

Cayleyjevo delovanje je posebni primer prostega delovanja – to je delovanje grupe G na množici X, za katero velja[4]

$$\forall g \in G - \{1\}\ \forall x \in X\colon\ g \cdot x \neq x.$$

Zgled.

- Cayleyjevo delovanje je prosto. Element $x \in G$ je namreč fiksna točka delovanja elementa $g \in G$, če in samo če velja $g \cdot x = x$, kar je mogoče le v primeru $g = 1$.
- Naj $\mathbb{Z}$ deluje na krožnici S^1 s predpisom

  $$\mathbb{Z} \to \mathrm{Isom}(S^1), \quad n \mapsto (z \mapsto z \cdot e^{2\pi i n \alpha})$$

  za nek izbrani parameter $\alpha \in \mathbb{R}$.

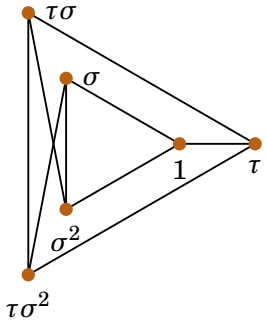
  - *Če je* $\alpha \in \mathbb{Q}$*:* Naj bo $\alpha = \frac{a}{b}$. Tedaj $n = b$ deluje kot id_{S^1}, torej delovanje *ni* prosto.
  - *Če je* $\alpha \in \mathbb{R} - \mathbb{Q}$*:* Število $z \in S^1$ je fiksna točka delovanja nekega $n \in \mathbb{Z}$, če in samo če je $2\pi i n \alpha \in 2\pi i \mathbb{Z}$, kar pomeni ravno $\alpha \in \mathbb{Q}$. Torej je za iracionalne izbire α to delovanje prosto.

Ko grupe delujejo na grafih, topoloških prostorih ali ostalih objektih različnih kategorij, pri definiciji prostega delovanja upoštevamo dodatno strukturo. Na primer, rečemo, da grupa G prosto deluje na grafu $\Gamma = (V, E)$, če velja:

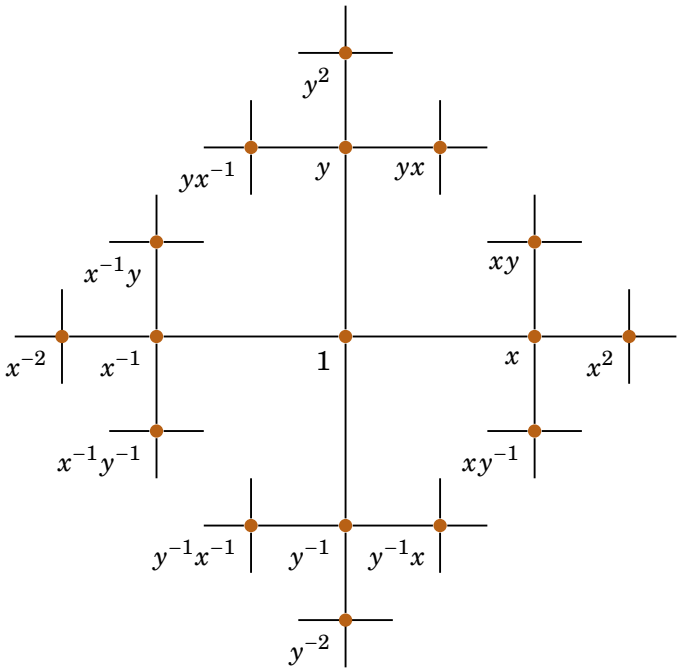
- obstaja homomorfizem $\rho\colon G \to \mathrm{Aut}(\Gamma)$, kjer grupa $\mathrm{Aut}(\Gamma)$ sestoji iz bijekcij $f\colon V \to V$, za katere velja

  $$\forall u, v \in V\colon\ \{u,v\} \in E \Leftrightarrow \{f(u), f(v)\} \in E,$$

[4] Pogoj pomeni, da noben netrivialen element grupe nima fiksnih točk.



Slika 2.5: $\mathrm{Cay}(S_3, \{\tau, \sigma\})$



Slika 2.6: $\mathrm{Cay}(F_2, \{x, y\})$

- za vsak $g \in G - \{1\}$ velja

$$\forall v \in V\colon \rho(g)(v) \neq v \quad \text{in} \quad \forall \{u,v\} \in E\colon \{\rho(g)(u), \rho(g)(v)\} \neq \{u,v\}.$$

Zgled. Grupa G deluje na grafu $\mathrm{Cay}(G,S)$:

$$G \to \mathrm{Aut}\,\mathrm{Cay}(G,S), \quad g \mapsto (x \mapsto g \cdot x).$$

Tukaj je pomembno, da smo v definiciji Cayleyjevega delovanja uporabili množenje z *leve* z elementom $g \in G$, v definiciji Cayleyjevega grafa pa smo uporabili množenje z *desne* z elementi $s \in S$.

Elementi $g \in G$ res delujejo kot avtomorfizmi grafa, ker za $x, y \in G$ velja:[5]

$$x \sim y \Leftrightarrow \exists s \in S \cup S^{-1}\colon x = y \cdot s \Leftrightarrow \exists s \in S \cup S^{-1}\colon g \cdot x = g \cdot y \cdot s \Leftrightarrow gx \sim gy.$$

To delovanje *ni* nujno vedno prosto. Na primer, če vzamemo $G = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$, $S = \{1\}$, potem je $\mathrm{Cay}(G,S)$ pot dolžine 1, na kateri element $1 \in G$

[5] Oznaka $x \sim y$ pomeni, da je x povezan z y v grafu $\mathrm{Cay}(G,S)$.

deluje tako, da zamenja vozlišči 0 in 1 med sabo in *ohranja povezavo* med njima.

Izkaže se, da je edina ovira za prostost delovanja grupe na svojem Cayleyjevem grafu obstoj elementov reda 2 v S.

Trditev. Bodi G grupa, $G = \langle S \rangle$. Cayleyjevo delovanje G na $\mathrm{Cay}(G,S)$ je prosto, če in samo če S *ne* vsebuje elementov reda 2.

Dokaz. Cayleyjevo delovanje je vselej prosto na vozliščih. Preveriti moramo le, kaj se dogaja s povezavami.

- *Če obstaja* $s \in S, s^2 = 1$*:* V tem primeru s deluje na povezavi $\{1,s\}$ tako, da jo preslika v povezavo $\{s,s^2\} = \{1,s\}$. Torej s fiksira to povezavo, zato delovanje *ni* prosto. ✓✓
- *Če delovanje ni prosto:* Naj bo $g \in G - \{1\}$, ki fiksira povezavo $\{u,v\}$. Velja torej $\{u,v\} = \{gu,gv\}$. Ker je $u \sim v$, lahko pišemo $v = us$ za nek $s \in S \cup S^{-1} - \{1\}$. Ločimo dva primera.
  - *Če je* $u = gu$ *in* $v = gv$*:* Sledi $g = 1$. Protislovje.
  - *Če je* $u = gv$ *in* $v = gu$*:* V tem primeru velja $u = gv = gus = vs = us^2$, zato sledi $s^2 = 1$. ✓✓

□

Orbite in stabilizatorji

Vsako delovanje G na množici X lahko razgradimo na *poddelovanja* na podmnožicah X. Osnovne enote so orbite. Orbita elementa $x \in X$ je množica $G.x = \{g.x \mid g \in G\}$.[6] Množica orbit je kvocientna množica $G\backslash X = \{G.x \mid x \in X\}$. Kadar ima X kakšno dodatno strukturo, ima ponavadi tudi množica orbit naravno dodatno strukturo.

Zgled. Naj grupa S^1 deluje na $\mathbb{C}$ s predpisom

$$S^1 \to \mathrm{Isom}(\mathbb{C}),\ z \mapsto (x \mapsto z \cdot x).$$

Velja $S^1.0 = \{0\}$, $S^1.i = S^1$. V splošnem je $S^1.x$ ravno krožnica s polmerom $|x|$. Kvocientno množico $S^1\backslash\mathbb{C}$ lahko naravno identificiramo z množico $\mathbb{R}_{\geq 0}$.

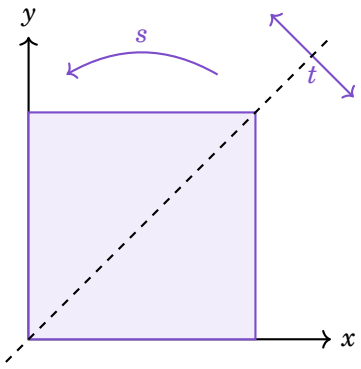
Stabilizator elementa $x \in X$ je $G_x = \{g \in G \mid g.x = x\}$. To je vselej podgrupa grupe G. Dualen objekt stabilizatorju je množica fiksnih točk dane podmnožice $H \subseteq G$, to je $X^H = \{x \in X \mid \forall h \in H\colon\ h.x = x\}$.

Zgled. Naj bo $K = [0,1] \times [0,1] \subseteq \mathbb{R}^2$ kvadrat. Grupa $G = \mathrm{Isom}(K)$ je izomorfna diedrski grupi D_8, generirana je z rotacijo $s\colon K \to K$ (vrtenje za $2\pi/4$) in zrcaljenjem $t\colon K \to K$ (zrcaljenje prek glavne diagonale $(0,0) - (1,1)$).

Fiksne točke generatorjev so $K^t = \{(x,x) \mid x \in [0,1]\}$, $K^s = \{(1/2,1/2)\}$. Velja še $G.(0,0) = \{(0,0),(1,0),(0,1),(1,1)\}$, $G_{(0,0)} = \{1,t\}$, $G_{(1/3,0)} = 1$, $K^G = \{(1/2,1/2)\}$. Točka $(1/2,1/2)$ je torej globalna fiksna točka delovanja.

Stabilizatorji in orbite so povezani na naslednji način.

[6] Grupa G deluje na X prek homomorfizma $\rho\colon G \to \mathrm{Sym}(X)$. Oznaka $g.x$ pomeni $\rho(g)(x)$.



Slika 2.7: Delovanja generatorjev diedrske grupe D_8 na kvadratu

Trditev. Naj G deluje na množici X. Naj bo $x \in X$. Tedaj je preslikava

$$A_x : G/G_x \to G.x, \quad gG_x \mapsto g.x$$

bijektivna, zato velja $|G/G_x| = |G.x|$. V primeru $|X|, |G| < \infty$ velja tudi

$$|G\backslash X| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Dokaz. A_x je dobro definirana: Če je $g_1 G_x = g_2 G_x$, potem $g_2^{-1} g_1 \in G_x$, zato $g_2^{-1} g_1 . x = x$, torej $g_2 . x = g_1 . x$. ✓✓

A_x je surjektivna: Velja po definiciji. ✓✓

A_x je injektivna: Če je $g_1 . x = g_2 . x$, potem $g_2^{-1} g_1 . x = x$, zato $g_2^{-1} g_1 \in G_x$, torej je $g_2 G_x = g_1 G_x$. ✓✓

Za zadnji del opazujmo množico $F = \{(g,x) \mid g \in G,\ x \in X,\ g.x = x\} \subseteq G \times X$. Velja $|F| = \sum_{g \in G} |X^g| = \sum_{x \in X} |G_x| = \sum_{x \in X} |G|/|G.x| = |G| \sum_{x \in X} 1/|G.x| = |G| \sum_{Y \in G\backslash X} \sum_{x \in Y} 1/|Y| = |G| \cdot |G\backslash X|$. ✓✓ □

Zgled. Naj bo p praštevilo, $C = \{x_1, \ldots, x_a\}$ za nek $a \in \mathbb{N}$ in naj bo $\mathcal{N} = C^p$ množica vseh nizov dolžine p iz črk C. Ciklična grupa $\mathbb{Z}/p\mathbb{Z}$ deluje na $\mathcal{N}$ s cikličnim zamikom:

$$\mathbb{Z}/p\mathbb{Z} \to \mathrm{Sym}(\mathcal{N}), \quad i \mapsto (c_1 \cdots c_p \mapsto c_{p-i+1} \cdots c_p c_1 \cdots c_{p-i}).$$

Število orbit tega delovanja je po zadnji trditvi enako

$$|\mathbb{Z}/p\mathbb{Z}\backslash\mathcal{N}| = \frac{1}{p} \sum_{i \in \mathbb{Z}/p\mathbb{Z}} |\mathcal{N}^i|.$$

Velja: $\mathcal{N}^0 = \mathcal{N}$ in za $i \neq 0$ je $\mathcal{N}^i = \{x_1 \cdots x_1, x_2 \cdots x_2, \ldots, x_a \cdots x_a\}$. Od tod sledi

$$|\mathbb{Z}/p\mathbb{Z}\backslash\mathcal{N}| = \frac{1}{p}(|\mathcal{N}^0| + (p-1)|\mathcal{N}^1|) = \frac{1}{p}(a^p + (p-1)a).$$

Ker velja $|\mathbb{Z}/p\mathbb{Z}\backslash\mathcal{N}| \in \mathbb{N}$, sledi $p \mid a^p + (p-1)a$, torej

$$\forall a \in \mathbb{Z}\colon\ a^p \equiv a \mod p.$$

To je natanko mali Fermatov izrek.

Tranzitivna delovanja

Delovanje grupe G na množici X je tranzitivno, če je $|G\backslash X| = 1$, torej če obstaja ena sama orbita.

Zgled. Opazujmo Cayleyjevo delovanje grupe G na $\mathrm{Cay}(G,S)$, kjer $\langle S\rangle = G$. To delovanje je vselej *tranzitivno na vozliščih*: za $x,y \in G$ element yx^{-1} preslika vozlišče x v y. To delovanje je tudi *prosto na vozliščih*: če je $gx = x$, potem sledi $g = 1$.

Izkaže se, da tranzitivnost in prostost *karakterizirata* Cayleyjeve grafe.

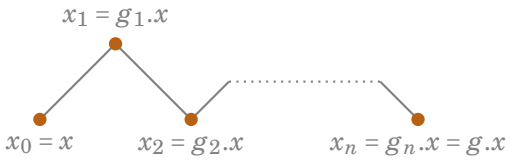
Trditev. Bodi G grupa, ki deluje na *povezanem* grafu $X = (V,E)$. Če je to delovanje tranzitivno in prosto na množici V, potem za vsak $x \in V$ velja, da množica $S = \{s \in G \mid \{x, s.x\} \in E\}$ generira G in $X \cong \mathrm{Cay}(G,S)$.

Dokaz. Definirajmo preslikavo $\varphi: G \to V, g \mapsto g.x$. Zaradi predpostavke o tranzitivnost in prostosti je φ bijekcija. Torej lahko identificiramo G in V prek φ.

S generira G: Naj bo $g \in G$. Opazujmo neko pot v grafu X od x do $g.x$:

$$x_0 = 0,\ x_1 = g_1.x,\ x_2 = g_2.x, \ldots, x_n = g_n.x = g.x.$$

za neke $g_i \in G$. Naj bo $s_j = g_j^{-1} \cdot g_{j+1}$.



Premislimo, da za vsak j velja $s_j \in S$: vemo $x_j \sim x_{j+1}$, zato je $g_j^{-1}.x_j \sim g_j^{-1}.x_{j+1}$, kar se poenostavi v $x \sim g_j^{-1} g_{j+1}.x \sim s_j.x$, torej je res $x \sim s_j.x$.

Zdaj velja $g = g_n = g_0 g_0^{-1} g_1 g_1^{-1} \cdots g_{n-1}^{-1} g_n = g_0 s_1 s_2 \cdots s_{n-1} = s_1 \cdots s_{n-1}$. Torej res S generira G. ✓✓

$X \cong \mathrm{Cay}(G,S)$: Imamo že bijekcijo med vozlišči obeh grafov, $\varphi: G \to V$. Za $g,h \in G$ velja $\varphi(g) \sim \varphi(h)$, če in samo če je $g.x \sim h.x$, kar je enakovredno $x \sim g^{-1}h.x$, torej $g^{-1}h \in S$, to pa je nazadnje enakovredno $g \sim h$ v $\mathrm{Cay}(G,S)$. Torej φ inducira izomorfizem grafov X in $\mathrm{Cay}(G,S)$. ✓✓ □

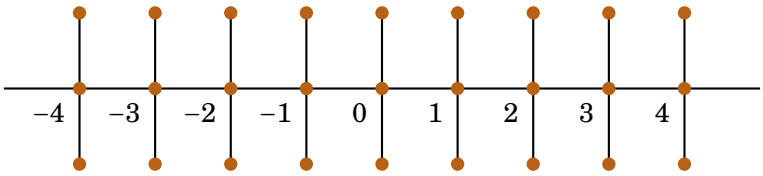
2.2 Proste grupe in drevesa

Prosto delovanje proste grupe na drevesu

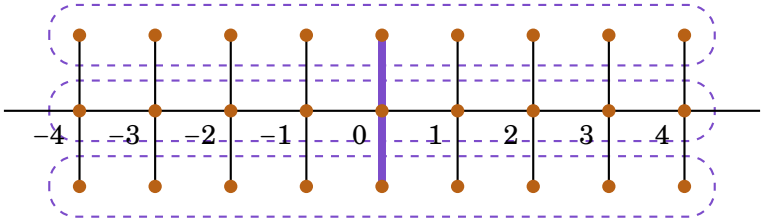
Bodi F prosta grupa, prosto generirana z množico $S \subseteq F$. Tedaj je $\mathrm{Cay}(F,S)$ drevo in F deluje na tem drevesu s Cayleyjevim delovanjem.

Ali je to delovanje prosto? Po trditvi iz prejšnjega razdelka vemo, da je temu tako, če in samo če S ne vsebuje elementov reda 2. Če obstaja $s_0 \in S$ reda 2, potem lahko definiramo preslikavo $S \to \mathbb{Z}$, ki preslika s_0 v 1, vse ostale elemente množice S pa v 0. Po univerzalni lastnosti proste grupe dobimo homomorfizem $\varphi: F \to \mathbb{Z}$ in velja račun $0 = \varphi(1) = \varphi(s_0^2) = \varphi(s_0)^2 = 2$. Protislovje. Torej tak s_0 ne obstaja in prosta grupa vselej deluje prosto na drevesu.

Dokazali bomo, da velja tudi obratno.



Slika 2.8: Drevo, na katerem prosto deluje grupa $\mathbb{Z}$ s pomikom v desno



Slika 2.9: Vpeto drevo delovanja $\mathbb{Z}$ in tri orbite na vozliščih drevesa

Izrek. (PROSTA ⇔ PROSTO NA DREVESU) Grupa je prosta, če in samo če deluje prosto na drevesu.

V eno smer smo izrek že premislili. Predpostavimo zdaj, da grupa G *prosto* deluje na (morda neskončnem) drevesu T.

Zgled. Grupa $\mathbb{Z}$ deluje s pomikom v desno na drevesu, ki ga dobimo tako, da v Cayleyjevem grafu $\mathrm{Cay}(\mathbb{Z}, \{1\})$ vsakemu vozlišču dodamo dva lista.

Kot vidimo v zadnjem zgledu, drevo T ni nujno Cayleyjev graf grupe G. Bomo pa pokazali, da lahko T vselej kontraktiramo oziroma skrčimo do Cayleyjevega grafa grupe G, in sicer tako, da kontraktiramo določena poddrevesa v T.

Vpeta drevesa delovanj

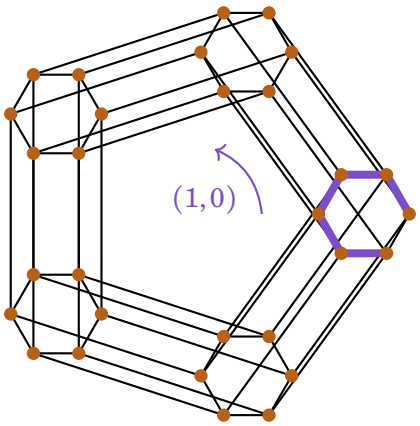
Naj grupa G deluje na grafu X z avtomorfizmi. Vpeto drevo delovanja G na X je podgraf X, ki je drevo in ki vsebuje natanko eno vozlišče v vsaki od G-orbit na vozliščih X.

Zgled.

- Naj $\mathbb{Z}$ deluje na drevesu s pomikom v desno kot v zadnjem zgledu. Imamo 3 orbite $\mathbb{Z}$ na vozliščih drevesa. Vpeto drevo je pot dolžine 2 od enega od novih listov prek vozlišča na Cayleyjevem grafu do drugega od listov.
- Grupa $\mathbb{Z}/n\mathbb{Z}$ deluje z rotacijo na diskretnem torusu $\mathrm{Cay}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, \{(1,0),(0,1)\})$. Število orbit na vozliščih je m. Vpeto drevo delovanja je v tem primeru m-cikel brez ene povezave.

Trditev. Vsako delovanje grupe na povezanem grafu ima vpeto drevo delovanja.

Dokaz. Naj G deluje na grafu X. Naj bo $\mathcal{T}$ množica vseh poddreves v X, ki vsebujejo največ eno vozlišče iz vsake G-orbite. Velja $\mathcal{T} \neq$, na primer $\mathcal{T}$ vsebuje drevo iz enega samega vozlišča. Množica $\mathcal{T}$ je delno urejena z relacijo inkluzije. Vsaka veriga v $\mathcal{T}$ ima zgornjo mejo (lahko vzamemo kar



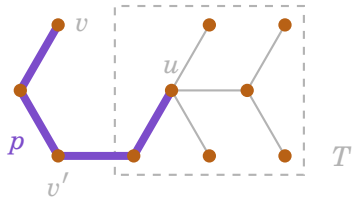
Slika 2.10: Vpeto drevo delovanja grupe $\mathbb{Z}/5\mathbb{Z}$ na diskretnem torusu $\mathrm{Cay}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \{(1,0),(0,1)\})$

unijo dreves v verigi). Po Zornovi lemi zato obstaja maksimalen element v $\mathcal{T}$: izberimo enega in mu recimo T.

T je vpeto drevo delovanja: Recimo, da ni. Torej obstaja $v \in V(X)$, da je $T \cap G.v = \emptyset$.

> Obstaja taka izbira v, da je v soseden nekemu vozlišču v T.

Dokaz: Ker je X povezan, obstaja pot p od nekega vozlišča $u \in T$ do v. Naj bo v' prvo vozlišče na p, ki ni v T.



- *Če $T \cap G.v' = \emptyset$:* V tem primeru lahko v nadomestimo z v'. 𝒻

- *Sicer:* V tem primeru obstaja $g \in G$, da je $g.v' \in T$. Naj bo p' odsek poti p od v' do v. Torej je $g.p'$ pot od $g.v' \in T$ do $g.v$, pri čemer velja $G.g.v \cap T = G.v \cap T = \emptyset$ po izbiri v. Torej je $g.p'$ krajša pot kot p z enako lastnostjo (povezuje T z vozliščem, katerega orbita ne seka T). Postopek ponavljamo in na koncu dobimo vozlišče z želeno lastnostjo. 𝒻

K drevesu T dodajmo izbrano vozlišče v in povezavo, ki ga povezuje z drevesom T. Dobimo novo drevo v $\mathcal{T}$, ki vsebuje T, kar je protislovje z maksimalnostjo drevesa $T \in \mathcal{T}$. Torej je res T vpeto drevo delovanja. 𝒻 □

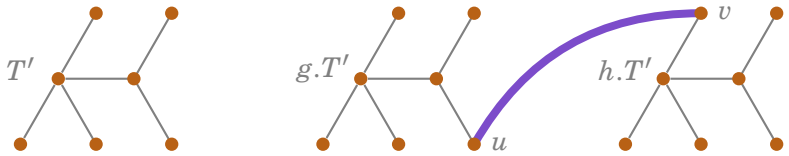
Kontrakcija in Cayleyjevo drevo

Dokaz izreka (PROSTA ⇔ PROSTO NA DREVESU)**.** Naj G deluje prosto na drevesu T. Dokazujemo, da je G prosta grupa.

Naj bo T' vpeto drevo delovanja G na T. Kontraktirajmo drevo T' v vozlišče, prav tako naredimo z orbitami T'. Na ta način dobimo nov graf X z:

- vozlišči $V = \{g.T' \mid g \in G\}$,
- povezavami $E = \{\{g.T', h.T'\} \mid g,h \in G,\ g.T' \text{ in } h.T' \text{ sta sosednji}\}$,

kjer sosednost $g.T'$ in $h.T'$ pomeni, da sta ti dve drevesi različni in da obstajata $u \in g.T'$, $v \in h.T'$ z $u \sim_T v$.



Za graf X veljajo naslednje lastnosti:

- Za vsaka različna elementa $g,h \in G$ je $g.T' \cap h.T' = \varnothing$. Ta lastnost sledi iz prostosti delovanja in izbire T'.
- Če sta $g.T', h.T'$ sosednji, potem med njima obstaja natako ena povezava v T. Ta lastnost velja, ker v T ni ciklov.
- Graf X je drevo. Cikel v X bi nam namreč porodil cikel v T.
- Grupa G inducirano deluje na X, to delovanje je tranzitivno in prosto na vozliščih X.

Iz zadnje lastnosti po dokazani trditvi sledi, da obstaja $\tilde{S} \subseteq G$, da je $X \cong \mathrm{Cay}(G,\tilde{S})$.

G nima elementov reda 2: Če je $s \in G$ reda 2, potem je $\langle s \rangle$ končna grupa, ki prosto deluje na drevesu T. To ni mogoče, saj ima vsako delovanje končne grupe na drevesu globalno fiksno točko (→ vaje). ✓✓

Ker v $\tilde{S}$ ni elementov reda 2, lahko izberemo $S \subseteq \tilde{S}$, za katero velja $S \cap S^{-1} = \varnothing$ in $\langle S \rangle = \langle \tilde{S} \rangle = G$. Še vedno je $\mathrm{Cay}(G,S)$ drevo. Iz trditve v razdelku o Cayleyjevem delovanju zdaj sledi, da S prosto generira G. □

Uporaba: podgrupe prostih grup

Posledica. (NIELSEN–SCHREIER) Podgrupa proste grupe je prosta.

Dokaz. Naj bo F prosta grupa in $G \leq F$. Grupa F prosto deluje na drevesu, zato tudi G prosto deluje na drevesu. Iz zadnjega izreka sledi, da je G prosta. □

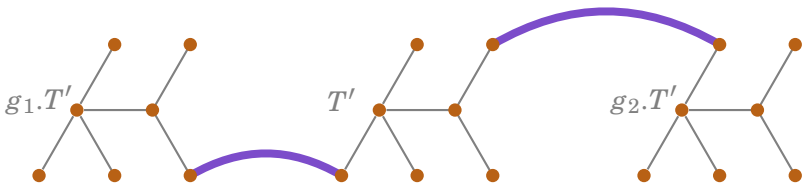
Zgled. Naj bo F_2 prosta grupa ranga 2, generirana z elementoma x,y. Opazujmo preslikavo $\{x,y\} \to S_3$, $x \mapsto (1\ 2), y \mapsto (1\ 2\ 3)$. Po univerzalni lastnosti obstaja razširitev te preslikave do homomorfizma $\varphi: F_2 \to S_3$. Ta je surjektiven, saj velja $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle$. Jedro $\ker\varphi$ je torej podgrupa indeksa 6 v F_2 in je zato sama prosta. Kateri prosti grupi je izomorfna grupa $\ker\varphi$?

Posledica. (KVANTITATIVNI NIELSEN–SCHREIER) Naj bo F prosta grupa ranga n in naj bo $G \leq F$ pogrupa indeksa k. Potem je G prosta ranga $k \cdot (n-1) + 1$.

Dokaz. Naj S prosto generira F. Naj bo $T = \mathrm{Cay}(F,S)$ drevo, na katerem F deluje prosto s Cayleyjevem delovanjem.

Opazujmo zožitev tega delovanja na podgrupo $G \leq F$. Naj bo T' vpeto drevo delovanja G na T. Za $f \in V(T) = F$ je orbita $G.f$ ravno desni odsek G v F, torej je število vozlišč v T' enako $|F : G| = k$.

Po kontrakciji poddreves $g.T'$ za $g \in G$ dobimo[7] drevo $X \cong \mathrm{Cay}(G,S')$ za nek $S' \subseteq G$ in grupa G je prosta ranga $|S'|$. Pri tem je $|S'|$ enako polovici[8] števila povezav od T' do $g.T'$ za vse $g \in G$.



Jasno velja

$$\sum_{v \in V(T')} \deg_T(v) = |V(T')| \cdot 2n = k \cdot 2n.$$

Po drugi strani pa lahko zadnjo vsoto izračunamo tako, da najprej upoštevamo notranje povezave v T', ki jih je natanko $2 \cdot (k-1)$ (vsako od $k-1$ povezav v T' preštejemo dvakrat), in za tem še povezave iz T' do drugih $g.T'$ za $g \in G$, ki jih je natanko $2 \cdot |S'|$. Sledi

$$|S'| = \frac{1}{2}(2kn - 2(k-1)) = k(n-1) + 1.$$

□

Zgled. Nadaljujemo zadnji zgled. Ker velja $|F_2 : \ker\varphi| = 6$, sledi $\ker\varphi \cong F_7$.

Posledica. Prosta grupa ranga vsaj 2 vsebuje proste podgrupe poljubno velikega ranga.

Dokaz. Sestavimo surjektiven homomorfizem $\varphi: F_r \to S_n = \langle (1\,2), (1\,2\,\cdots\,n) \rangle$. Jedro $\ker\varphi$ je prosta grupa ranga $n! \cdot (r-1) + 1$, kar raste čez vse meje ko gre $n \to \infty$. Hkrati $\ker\varphi$ vsebuje proste grupe vsakega ranga manjšega od $n!(r-1)+1$. □

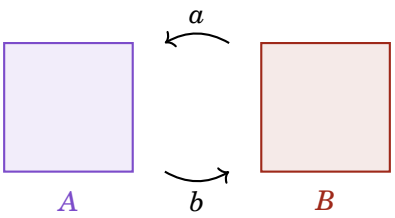
Posledica. Podgrupa končnega indeksa v končno generirani grupi je končno generirana.

Dokaz. Naj bo G končno generirana grupa in naj bo $H \leq G$ podgrupa končnega indeksa. Naj bo $G = \langle S \rangle$, $|S| < \infty$. Naj bo $\pi: F(S) \to G$ surjektiven homomorfizem. Naj bo $H' = \pi^{-1}(H) \leq F(S)$. Velja $|F(S) : H'| = |F(S)/\ker\pi : H'/\ker\pi| = |G : H| < \infty$. Torej je H' končno generirana prosta grupa. Njena slika $H = \pi(H')$ je zato tudi končno generirana. □

Premislek pokaže (→ vaje), da je število podgrup danega indeksa v končno generirani grupi G vselej končno, njihov presek pa je podgrupa edinka končnega indeksa v G.

[7] Kot v dokazu izreka (PROSTA ⇔ PROSTO NA DREVESU).

[8] V Cayleyjevem grafu imamo namreč dve povezavi za vsak $s \in S'$: s in s^{-1}.



Slika 2.11: Pingpong

Pingpong

Vzpostavili bomo še en geometrijski kriterij za prepoznavanje prostih grup.

Izrek. (PINGPONG) Naj bo $G = \langle a, b \rangle$ grupa z delovanjem na množici X. Predpostavimo, da obstajata neprazni podmnožici $A, B \subseteq X$, $B \nsubseteq A$, ki zadoščata *pingpong pogoju*:

$$\forall n \in \mathbb{Z}\backslash\{0\}\colon\ a^n.B \subseteq A \text{ in } b^n.A \subseteq B.$$

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

Dokaz. Naj bo $F = F(\{\alpha, \beta\})$ prosto generirana s simboloma α, β. Po univerzalni lastnosti dobimo homomorfizem $\varphi\colon F \to G$, $\alpha \mapsto a, \beta \mapsto b$. Predpostavimo, da φ *ni* injektiven. Naj bo torej $w \in F$ okrajšana beseda v $\ker\varphi$. Obravnavajmo štiri možnosti glede na začetek in konec besede w.

- *w se začne in konča z α:* V tem primeru je $w = \alpha^{n_0}\beta^{m_1}\alpha^{n_1}\cdots\beta^{m_k}\alpha^{n_k}$ za $n_i, m_i \in \mathbb{Z}\backslash\{0\}$. Jasno je $\varphi(w).B = B$, po drugi strani pa po pingpong pogoju velja

  $$\varphi(w).B = a^{n_0}b^{m_1}a^{n_1}\cdots b^{m_k}a^{n_k}.B \subseteq a^{n_0}b^{m_1}a^{n_1}\cdots b^{m_k}.A \subseteq \cdots \subseteq a^{n_0}.B \subseteq A.$$

  Protislovje s predpostavko $B \nsubseteq A$.

- *w se začne in konča z β:* V tem primeru je konjugirana beseda $\alpha w \alpha^{-1}$ okrajšana beseda v jedru $\ker\varphi$, ki je enake oblike kot v prvem primeru. Protislovje.

- *w se začne z α in konča z β:* V tem primeru je $w = \alpha^n w' \beta^m$ za $n, m \in \mathbb{Z}\backslash\{0\}$. Tako je konjugirana beseda $\alpha^k w \alpha^{-k} = \alpha^{k+n} w' \beta^m \alpha^{-k}$ okrajšana beseda v $\ker\varphi$, ki je enake oblike kot v prvem primeru. Protislovje.

- *w se začne z β in konča z α:* V tem primeru je w^{-1} okrajšana beseda v $\ker\varphi$, ki je kot v tretjem primeru. Protislovje.

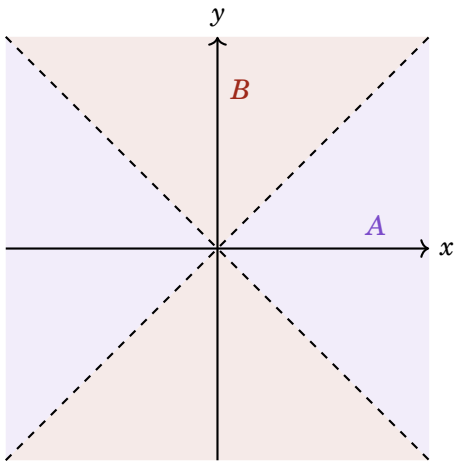
□

Zgled. Opazujmo grupo matrik $\mathrm{SL}_2(\mathbb{Z}) = \{A \in \mathrm{GL}_2(\mathbb{Z}) \mid \det A = 1\}$. Izberimo njuna elementa

$$a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Dokažimo, da je $\langle a, b \rangle$ prosta grupa, prosto generirana z $\{a, b\}$. V ta namen uporabimo (PINGPONG). Grupa $\mathrm{SL}_2(\mathbb{Z})$ naravno deluje na ravnini $\mathbb{R}^2$. Razdelimo jo na dva dela:

$$A = \{(x, y) \in \mathbb{R}^2 \mid |x| > |y|\}, \quad B = \{(x, y) \in \mathbb{R}^2 \mid |x| < |y|\}.$$



Slika 2.12: Pingpong v ravnini $\mathbb{R}^2$ glede na delovanje grupe $\mathrm{SL}_2(\mathbb{Z})$

Za vsak $n \in \mathbb{Z}\setminus\{0\}$ in $(x,y) \in B$ velja

$$a^n \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+2ny \\ y \end{pmatrix} \in A,$$

kjer zadnja vsebovanost sledi iz $|x+2ny| \geq |2ny|-|x| \geq 2|y|-|x| > 2|y|-|y| = |y|$. Torej je res $a^n.B \subseteq A$. Podobno preverimo $b^n.A \subseteq B$.

Z nekaj dodatnega premisleka se da pokazati (→ vaje), da velja celo $|\mathrm{SL}_2(\mathbb{Z}) : \langle a,b\rangle| = 12$. Torej $\mathrm{SL}_2(\mathbb{Z})$ vsebuje prosto podgrupo končnega indeksa.

Naj bo $\mathcal{P}$ grupno-teoretična lastnost.[9] Če ima grupa G podgrupo H, ki zadošča $\mathcal{P}$ in je končnega indeksa v G, potem rečemo, da G virtualno zadošča $\mathcal{P}$.

Zgled.

- $\mathrm{SL}_2(\mathbb{Z})$ je virtualno prosta grupa.
- Iz kvantitativnega Nielsen–Schreierjevega izreka sledi, da je prosta grupa ranga 2 virtualno prosta ranga k za vsak $k \geq 2$.
- Vsaka končna grupa je virtualno trivialna.

[9] Na primer, $\mathcal{P}$ je lahko *je abelova grupa* ali *je prosta grupa*.

Poglavje 3

Struktura grup

V tem razdelku si bomo ogledali, kako lahko grupe *razrežemo* na preproste kose.

3.1 Rešljive grupe

Rešljivost

Grupa G je rešljiva, če ima verigo podgrup

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1,$$

katerih faktorji G_i/G_{i+1} so abelovi za vsak $i = 1,2,\ldots,n-1$. Ekvivalentno, velja $\forall x,y \in G_i\colon\ [x,y] \in G_{i+1}$. Rešljive grupe so torej grupe, ki jih lahko *razrežemo* na abelove kose.

Za podgrupi $H,K \leq G$ uvedimo oznako

$$[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle.$$

Pogoj, da je G_i/G_{i+1} abelova, je ekvivalenten $[G_i,G_i] \leq G_{i+1}$.

Izvedena vrsta

V grupi G induktivno definiramo njeno izvedeno vrsto podgrup

$$G^{(1)} = G, \quad G^{(i+1)} = [G^{(i)},G^{(i)}] \text{ za } i \geq 1.$$

Premislimo naprej, da velja $G^{(i+1)} \trianglelefteq G^{(i)}$. Naj bo $w \in G^{(i+1)}$, torej $w = \prod_j [a_j,b_j]$ za neke $a_j,b_j \in G^{(i)}$. Za vsak $g \in G^{(i)}$ tedaj velja

$$gwg^{-1} = \prod_j g[a_j,b_j]g^{-1} = \prod_j [ga_jg^{-1},gb_jg^{-1}] \in \prod_j [G^{(i)},G^{(i)}] \subseteq G^{(i+1)}.$$

Opazimo, da je po definiciji grupa $G^{(i)}/G^{(i+1)}$ vselej abelova. Če torej za nek $n \in \mathbb{N}$ velja $G^{(n)} = 1$, potem je G rešljiva. Res pa je tudi obratno.

Trditev. Grupa G je rešljiva, če in samo če velja $G^{(n)} = 1$ za nek $n \in \mathbb{N}$.

Dokaz. Predpostavimo, da je G rešljiva in da njeno rešljivost opazi veriga $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$. Velja torej $[G_i,G_i] \leq G_{i+1}$ za vsak i. Sledi $G^{(1)} = G_1$, $G^{(2)} = [G_1,G_1] \leq G_2$, $G^{(3)} = [G^{(2)},G^{(2)}] \leq [G_2,G_2] \leq G_3$,

... Induktivno sklepamo, da za vsak i velja $G^{(i)} \leq G_i$. Zato mora veljati tudi $G^{(n)} = 1$. □

Najmanjše število $n \in \mathbb{N}$ z lastnostjo $G^{(n+1)} = 1$ je izvedena dolžina grupe G.

Zgled.

- Abelova grupa je rešljiva izvedene dolžine 1.
- Opazujmo diedrsko grupo $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong \langle s,t \mid s^n, t^2, tst^{-1} = s^{-1} \rangle$. Velja $[s,t] = s^{-2} \in D_{2n}^{(2)}$, zato $\langle s^2 \rangle \in D_{2n}^{(2)}$. Predpostavimo, da je n sodo število. Tedaj je kvocient $D_{2n}/\langle s^2 \rangle$ izomorfen grupi $\langle s,t \mid s^2, t^2, tst^{-1} = s^{-1} \rangle = \langle s,t \mid s^2, t^2, st = ts \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ker je slednja grupa abelova, od tod sledi $D_{2n}^{(2)} \leq \langle s^2 \rangle$ in zato velja $D_{2n}^{(2)} = \langle s^2 \rangle$. Slednja grupa je abelova, zato je nazadnje $D_{2n}^{(3)} = 1$. Torej je D_{2n} rešljiva izvedene dolžine 2. Če je n liho število, podoben argument pokaže, da je $D_{2n}^{(2)} = \langle s^2 \rangle = \langle s \rangle$ in $D_{2n}^{(3)} = 1$, torej je tudi v tem primeru grupa rešljiva izvedene dolžine 2.

S pomočjo izvedene vrste lahko preprosto izpeljemo dednost rešljivosti v osnovnih primerih konstrukcij novih grup.

Trditev. Podgrupe in kvocienti rešljivih grup so rešljivi. Razširitev rešljive grupe z rešljivo je rešljiva.

Dokaz. Naj bo G rešljiva grupa z $G^{(n)} = 1$.

Za podgrupo $H \leq G$ preprost induktiven argument dokaže $H^{(i)} \leq G^{(i)}$ za vsak i. V posebnem sledi $H^{(n)} = 1$. ✓✓

Za $N \trianglelefteq G$ velja $(G/N)^{(n)} = G^{(n)}N/N = 1$. ✓✓

Naj bo nazadnje K še ena rešljiva grupa z $K^{(m)} = 1$. Naj bo E razširitev K z G. Tedaj velja $E^{(m)}G/G = (E/G)^{(m)} = K^m = 1$, zato je $E^{(m)} \leq G$. Od tod induktivno sledi $E^{(m+i)} \leq G^{(i)}$ za vsak i, zato v posebnem velja $E^{(m+n)} = 1$. ✓✓ □

Zgled. Svetilkarjeva grupa $L = (\bigoplus_{i \in \mathbb{Z}} \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}$ je razširitev abelove grupe z abelovo, torej je rešljiva.

Noetherskost

Trditev. Bodi G grupa. Naslednje trditve so ekvivalentne:

1. Vsaka neprazna množica podgrup grupe G ima maksimalen element.
2. Vsaka strogo naraščajoča veriga podgrup $G_1 < G_2 < \cdots$ grupe G je končna.
3. Vsaka podgrupa grupe G je končno generirana.

Grupe, ki zadoščajo tem pogojem, imenujemo noetherske.

Dokaz. 1. $\Rightarrow$ 2.: Imejmo verigo $G_1 < G_2 < \cdots$ v G. Tedaj ima množica $\{G_1, G_2, \ldots\}$ po predpostavki maksimalen element. Torej je veriga končna. ✓✓

2. $\Rightarrow$ 1.: Uporabimo Zornovo lemo. Ker ima vsaka veriga zgornjo mejo (namreč, zadnji člen verige), obstaja maksimalen element katerekoli množice podgrup. ✓✓

2. $\Rightarrow$ 3.: Naj bo $H \leq G$. Izberimo neko množico generatorjev S grupe H. Naj bo $s_1 \in S$ in $H_1 = \langle s_1 \rangle$. Če je $H_1 = H$, je H končno generirana. Predpostavimo zdaj $H_1 < H$. Naj bo $s_2 \in S \setminus H_1$ in $H_2 = \langle s_1, s_2 \rangle$. Če je $H_2 = H$, je H končno generirana. Predpostavimo zdaj $H_1 < H_2 < H$. Postopek nadaljujemo in dobimo naraščajočo verigo podgrup v H. Ker je vsaka veriga v G končna, se mora ta postopek ustaviti. Torej obstaja $i \in \mathbb{N}$, da je $H_i = H$. S tem je $H = \langle s_1, s_2, \ldots, s_i \rangle$. $\lightning$

3. $\Rightarrow$ 2.: Naj bo $G_1 < G_2 < \cdots$ neskončna veriga v G. Naj bo $H = \bigcup_{i \in \mathbb{N}} G_i$. Velja $H \leq G$, zato je po predpostavki $H = \langle h_1, \cdots, h_n \rangle$ za neke $h_i \in H$. Za vsak generator h_i obstaja člen verige, ki ga vsebuje. Torej obstaja člen verige, recimo G_k, ki vsebuje vse $h_1, \ldots, h_n$. Torej $G_k \geq H$, zato je $G_i \leq G_k$ za vsak $i \in \mathbb{N}$. Veriga je torej končna. Protislovje. $\lightning$ □

Ni se težko prepričati (→ vaje), da je lastnost noetherskosti zaprta za podgrupe, kvociente in razširitve.

Zgled.

- $\mathbb{Z}$ je noetherska grupa.
- Končne grupe so noetherske.
- Iz zgodnjih dveh primerov sledi, da je vsaka končno generirana abelova grupa noetherska.
- $\mathbb{Q}$ ni noetherska grupa. Vsebuje namreč podgrupe $H_k = \{ \frac{a}{2^i} \mid a \in \mathbb{Z},\ i \in \mathbb{N}_0,\ i \leq k \}$ za $k \in \mathbb{N}_0$, ki tvorijo neskončno verigo

$$\mathbb{Z} = H_0 < H_1 < H_2 < \cdots < \mathbb{Q}.$$

Trditev. Rešljiva grupa je noetherska, če in samo če ima verigo

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1,$$

kjer so vsi kvocienti G_i/G_{i+1} *ciklični*.

Rešljivim noetherskim grupam pravimo policiklične.

Dokaz. ($\Leftarrow$): Ciklične grupe so noetherske. Tako je najprej G_{n-1} noetherska. Ker je G_{n-2} razširitev ciklične grupe G_{n-2}/G_{n-1} z grupo G_{n-1}, je tudi G_{n-2} noetherska. Induktivno na ta način sklepamo, da je G_i noetherska za vsak i. V posebnem je $G = G_1$ noetherska. $\lightning$

($\Rightarrow$): Bodi G rešljiva z verigo $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$ z abelovimi kvocienti. Ker je G noetherska, je noetherski tudi vsak člen verige G_i, zato je G_i/G_{i+1} noetherska, torej je nazadnje G_i/G_{i+1} končno generirana abelova grupa. Zapišemo jo lahko kot direktno vsoto cikličnih grup:

$$G_i/G_{i+1} = C_1 \oplus C_2 \oplus \cdots \oplus C_k.$$

Naj bo $H_\ell = \left(\bigoplus_{j=1}^{\ell} C_j \right) G_{i+1} \leq G_i$ delna vsota cikličnih podgrup, dvignjena v grupo G_i. Torej imamo verigo podgrup

$$G_{i+1} = H_0 \leq H_1 \leq \cdots \leq H_k = G_i$$

s kvocienti $H_{j+1}/H_j \cong C_{j+1}$. Na ta način lahko v grupi G originalno verigo med vsakima členoma $G_{i+1} \trianglelefteq G_i$ pofinimo z vmesnimi podgrupami H_j, tako da so v novi verigi vsi kvocienti ciklični. Torej je G policiklična. $\lightning$ □

Zgled.

- $\mathbb{Q}$ ni noetherska, torej ni policiklična grupa.
- Svetilkarjeva grupa L ima podgrupo $\bigoplus_{i\in\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, ki *ni* končno generirana. Torej L *ni* noetherska.
- Končne rešljive grupe so policiklične, na primer D_{2n} je policiklična.
- Neskončna diedrska grupa $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ je policiklična.

Hirschova dolžina

Lema. Naj ima grupa G dve verigi podgrup:

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1 \quad (G\text{-veriga})$$

in

$$G = H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_m = 1. \quad (H\text{-veriga})$$

Tedaj obstajata verigi podgrup

$$G = K_{1,1} \trianglerighteq K_{1,2} \trianglerighteq \cdots \trianglerighteq K_{1,n} \trianglerighteq K_{2,1} \trianglerighteq \cdots \trianglerighteq K_{m,n} = 1 \quad (K\text{-veriga})$$

in

$$G = L_{1,1} \trianglerighteq L_{1,2} \trianglerighteq \cdots \trianglerighteq L_{1,m} \trianglerighteq L_{2,1} \trianglerighteq \cdots \trianglerighteq L_{n,m} = 1, \quad (L\text{-veriga})$$

pri čemer je K-veriga pofinitev H-verige (= vsi členi H-verige se pojavijo v K-verigi), L-veriga je pofinitev G-verige in kvocienti K-verige so do permutacije členov natančno enaki kvocientom L-verige.

Dokaz. Pofinimo H-verigo s pomočjo G-verige. Najprej velja

$$G = H_1 \trianglerighteq H_2G_2 \trianglerighteq H_2G_3 \trianglerighteq \cdots \trianglerighteq H_2G_n = H_2,$$

za tem imamo verigo

$$H_2 \trianglerighteq H_3(G_2 \cap H_2) \trianglerighteq H_3(G_3 \cap H_2) \trianglerighteq \cdots \trianglerighteq H_3(G_n \cap H_2) = H_3,$$

med splošnima členoma $H_i \trianglerighteq H_{i+1}$ pa imamo verigo

$$H_i \trianglerighteq H_{i+1}(G_2 \cap H_i) \trianglerighteq H_{i+1}(G_3 \cap H_i) \trianglerighteq \cdots \trianglerighteq H_{i+1}(G_n \cap H_i) = H_{i+1}.$$

Označimo $K_{i,j} = H_{i+1}(G_j \cap H_i)$. Tako dobimo K-verigo,

$$G = K_{1,1} \trianglerighteq K_{1,2} \trianglerighteq \cdots \trianglerighteq K_{m,n} = 1,$$

ki je pofinitev H-verige, saj velja $K_{i,1} = H_i$.

Analogno lahko pofinimo G-verigo s pomočjo H-verige. Naj bo $L_{j,i} = G_{j+1}(H_i \cap G_j)$. Tako dobimo L-verigo,

$$G = L_{1,1} \trianglerighteq L_{1,2} \trianglerighteq \cdots \trianglerighteq L_{n,m} = 1,$$

ki je pofinitev G-verige, saj velja $L_{j,1} = G_j$.

Obe novi verigi imata enako število členov $(n \cdot m)$. Za kvociente K-verige velja

$$K_{i,j}/K_{i,j+1} = \frac{H_{i+1}(G_j \cap H_i)}{H_{i+1}(G_{j+1} \cap H_i)} \cong \frac{H_{i+1}(G_j \cap H_i)/H_{i+1}}{H_{i+1}(G_{j+1} \cap H_i)/H_{i+1}}.$$

Zdaj uporabimo drugi izrek o izomorfizmu[1], od koder sledi

$$K_{i,j}/K_{i,j+1} \cong \frac{(G_j \cap H_i)/(G_j \cap H_{i+1})}{(G_{j+1} \cap H_i)(G_j \cap H_{i+1})/(G_j \cap H_{i+1})} \cong \frac{G_j \cap H_i}{(G_{j+1} \cap H_i)(G_j \cap H_{i+1})}.$$

Zadnja grupa je simetrična glede na menjavo G-vrste in H-vrste. Torej bi do enakega rezultata prišli z analizo kvocientov L-vrste. Od tod sledi

$$K_{i,j}/K_{i,j+1} \cong L_{j,i}/L_{j,i+1}.$$

Dokaz je s tem zaključen. □

Trditev. Bodi G policiklična grupa. Vsaki verigi, ki opazita policikličnost G, imata enako število neskončnih kvocientov.

Dokaz. Po lemi imata vsaki dve verigi pofinitev z enakimi cikličnimi kvocienti (do permutacije natančno). Zato je trditev dovolj dokazati za primer, ko je prva veriga pofinitev druge. Tako pofinitev dobimo z zaporednim vstavljanjem enega novega člena med dva obstoječa: $G_i < H < G_{i-1}$. Ločimo dva primera.

- *Če je* $|G_{i-1}/G_i| < \infty$*:* V tem primeru ima nova veriga (z dodanim členom H) enako število neskončnih kvocientov. 𝒻𝒻
- *Če je* $G_{i-1}/G_i \cong \mathbb{Z}$*:* V tem primeru je nujno $H/G_i \cong \mathbb{Z}$ in $|G_{i-1}/H| < \infty$. Torej je število neskončnih kvocientov v stari in novi verigi zopet enako. 𝒻𝒻

□

Število neskončnih kvocientov v katerikoli verigi policiklične grupe G se imenuje Hirschova dolžina, oznaka $h(G)$.

Zgled.

- Hirschova dolžina $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ je enaka $h(D_\infty) = 1$.
- Opazujmo Heisenbergovo grupo

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a,b,c \in \mathbb{Z} \right\} \leq \mathrm{GL}_3(\mathbb{Z}).$$

  Ta grupa je policiklična, kar opazi veriga podgrup

$$H \trianglerighteq \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid a,b \in \mathbb{Z} \right\} \trianglerighteq \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z} \right\} \trianglerighteq 1.$$

  Kvocienti te verige so vsi izomorfni $\mathbb{Z}$. Torej je $h(H) = 3$.

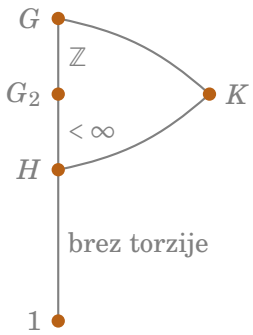
Hirschova dolžina je pomembna invarianta policikličnih grup, ki jo lahko uporabimo pri induktivnih sklepih. Primer take uporabe je podan v naslednji trditvi. Rečemo, da je grupa brez torzije, kadar nima netrivialnih elementov končnega reda.

[1] Natančneje, za grupe X, Y, Z, $Z \leq X$, velja $XY/Y \cong X/(X \cap Y)$, ta izomorfizem pa prenese podgrupo ZY/Y v $Z(X \cap Y)/(X \cap Y)$.

Trditev. Policiklične grupe so virtualno brez torzije.

Dokaz. Indukcija na Hirschovo dolžino. Naj bo $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = 1$. Naj bo G_i/G_{i+1} prvi neskončni kvocient te vrste. Torej je $|G : G_i| < \infty$. Dovolj bo zato dokazati, da je policiklična grupa G_i virtualno brez torzije. Brez škode za splošnost lahko torej privzamemo $i = 1$.

Ker velja $h(G_2) = h(G) - 1$, po indukciji obstaja $H \leq G_2$, za katero je $|G_2 : H| < \infty$ in H je brez torzije. Privzamemo lahko, da je $H \trianglelefteq G$.[2] Naj bo $G/G_2 = \langle xG_2 \rangle$ za nek $x \in G$. Naj bo $K = \langle x, H \rangle$.



K je končnega indeksa v G: Velja $G = KG_2$, zato je $|G : K| = |G_2K : K| = |G_2 : G_2 \cap K| \leq |G_2 : H| < \infty$.

K je brez torzije: Vsak element $k \in K$ lahko zapišemo kot $k = x^a h$ za neka $a \in \mathbb{Z}$ in $h \in H$. Če je k torzijski element, potem je $k^m = 1$, od koder sledi $H = k^m H = (kH)^m = x^{am} H$, zato je $x^{am} \in H \leq G_2$. V tem primeru je xG_2 reda največ am v $G/G_2 \cong \mathbb{Z}$. Od tod sledi $a = 0$. Tako je $k = h \in H$. Ker je H brez torzije, je slednje sprto s predpostavko, da je k torzijski element. ✓✓ □

3.2 Nilpotentne grupe

Nilpotentnost

Grupa G je nilpotentna, če ima verigo podgrup

$$G = G_1 \geq G_2 \geq \cdots \geq G_n = 1$$

z lastnostjo $G_i \trianglelefteq G$ in $G_i/G_{i+1} \leq Z(G/G_{i+1})$[3] za vsak $i = 1, 2, \ldots, n-1$. Taki verigi rečemo centralna vrsta.

Pogoj $G_i/G_{i+1} \leq Z(G/G_{i+1})$ je ekvivalenten $\forall x \in G_i \ \forall g \in G\colon [x, g] \in G_{i+1}$, kar lahko krajše zapišemo kot $[G_i, G] \leq G_{i+1}$.

Nilpotentne grupe so jasno rešljive.

Spodnja in zgornja centralna vrsta

Kot pri rešljivosti lahko opazimo nilpotentnost z eno posebno verigo. Induktivno definiramo spodnjo centralno vrsto z naslednjim predpisom:

$$\gamma_1(G) = G, \quad \gamma_{i+1}(G) = [\gamma_i(G), G] \text{ za } i \geq 1.$$

[2] Po potrebi namreč lahko H zamenjamo s presekom $\bigcap_{K \leq G, |G:K| = |G:H|} K$, ki je edinka končnega indeksa v G.

[3] Center grupe G je $Z(G) = \{x \in G \mid \forall y \in G\colon xy = yx\}$.

Induktivno hitro preverimo, da za vsako centralno vrsto $G = G_1 \geq G_2 \geq \cdots \geq G_n = 1$ velja $\gamma_i(G) \leq G_i$, zato sledi $\gamma_n(G) = 1$. Res je tudi obratno. Če je $\gamma_c(G) = 1$ za nek c, potem je $G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_c(G) = 1$ centralna vrsta, ki opazi nilpotentnost grupe G. Torej je G nilpotentna, če in samo če velja $\gamma_c(G) = 1$ za nek c. Če je c najmanjše število s to lastnostjo, potem rečemo, da je G razreda nilpotentnosti $c-1$.

Zgled.

- Grupe razreda nilpotentnosti 1 so natanko grupe z $\gamma_2(G) = 1$, kar je ekvivalentno $[G,G] = 1$, torej so to natanko abelove grupe.
- Naj bo H Heisenbergova grupa. Izračunamo

$$\gamma_2(H) = H^{(2)} = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z} \right\} \leq Z(H).$$

  Torej je $\gamma_3(H) = [\gamma_2(H), H] = 1$. Tako je H nilpotentna razreda 2.

Analogno definiramo zgornjo centralno vrsto z naslednjim predpisom:

$$Z_1(G) = Z(G), \quad Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)) \text{ za } i \geq 1.$$

Induktivno hitro sledi, da za vsako centralno vrsto $G = G_1 \geq G_2 \geq \cdots \geq G_n = 1$ velja $Z_i(G) \geq G_{n-i}$, zato sledi $Z_{n-1}(G) = G$. Res je tudi obratno. Če je $Z_c(G) = G$ za nek c, potem je $G = Z_c(G) \geq Z_{c-1}(G) \geq \cdots \geq Z_1(G) \geq 1$ centralna vrsta, ki opazi nilpotentnost grupe G. Torej je G nilpotentna, če in samo če velja $Z_c(G) = G$ za nek c. Najmanjši tak c je ravno razred nilpotentnosti grupe G (→ vaje).

Zgled.

- Če je G abelova grupa, potem je $Z_1(G) = G$. Razred nilpotentnosti G je enak 1.
- Naj bo H Heisenbergova grupa. Izračunamo

$$Z_1(H) = Z(H) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z} \right\} = \gamma_2(H).$$

  Hkrati je $H/Z(H) \cong \mathbb{Z} \times \mathbb{Z}$, torej je $Z_2(H) = H$. Razred nilpotentnosti grupe H je enak 2.
- Členi spodnje in zgodnje centralne vrste niso nujno enaki. Naj bo na primer $G = H \times \mathbb{Z}$, kjer je H Heisenbergova grupa. Tedaj je $\gamma_2(G) = \gamma_2(H) \times 1$, $Z_1(G) = Z(H) \times \mathbb{Z} = \gamma_2(H) \times \mathbb{Z}$.

Kot pri rešljivih grupah ni težko preveriti, da so nilpotente grupe zaprte za podgrupe, kvociente in direktne produkte (→ vaje).

Zgled. Nilpotentne grupe *niso* nujno zaprte za razširitve. Preprost primer je simetrična grupa S_3, katere veriga $S_3 \geq A_3 \cong \mathbb{Z}/3\mathbb{Z} \geq 1$ s kvocientom $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ opazi njeno policikličnost. Ker velja $Z(S_3) = 1$, grupa S_3 ni nilpotentna.

Zgled. Velik razred nilpotentnih grup tvorijo končne p-grupe.[4] To so grupe, katerih moč je potenca praštevila p. Razlog za njihovo nilpotentost

[4] Kasneje bomo pojasnili, kaj točno mislimo z izrazom, da končne p-grupe tvorijo *velik* razred grup.

je v tem, da imajo take grupe vselej netrivialen center. V taki grupi G zato velja $Z_1(G) > 1$, $Z_2(G)/Z_1(G) = Z(G/Z_1(G)) > Z_1$, ... in torej zgornja centralna vrsta strogo raste, če še ni dosegla celotne grupe G. Slej kot prej torej velja $Z_c(G) = G$ za nek c.

Komutatorji

Komutator elementov $x, y \in G$ je $[x,y] = x^{-1}y^{-1}xy$. Preprost račun pokaže, da komutator zadošča naslednjima komutatorskima identitetama:

$$[xy,z] = [x,z]^y \cdot [y,z],$$
$$[x,yz] = [x,z] \cdot [x,y]^z,$$

pri čemer smo uporabili oznako $g^x = x^{-1}gx$ za desno konjugiranje.[5]

V nilpotentni grupi G razreda 2 velja $\gamma_2(G) \leq Z(G)$, zato je v taki grupi res $[xy,z] = [x,z][y,z]$ in $[x,yz] = [x,y][x,z]$, torej je komutator *bilinearen* v taki grupi.

Komutator uteži c je element $[x_1,x_2,\ldots,x_c]$, definiran induktivno kot

$$[x_1,x_2,\ldots,x_c] = [[x_1,x_2,\ldots,x_{c-1}],x_c].$$

Komutatorji uteži 1 so običajni grupni elementi. Komutatorji uteži 2 so običajni komutatorji dveh grupnih elementov. Komutator uteži 3 pa je na primer element $[x,y,z] = [[x,y],z] = [x,y]^{-1}z^{-1}[x,y]z$.

Preprost račun pokaže, da za komutatorje uteži 3 v vsaki grupi velja Hall-Wittova identiteta:[6]

$$[x,y^{-1},z]^y \cdot [y,z^{-1},x]^z \cdot [z,x^{-1},y]^x = 1.$$

Analogno oznako kot za komutatorje višjih uteži uporabimo za podgrupe. Za podgrupe $H,K,L \leq G$ imamo torej $[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle$ in $[H,K,L] = [[H,K],L]$. Pri tem moramo biti previdni, saj je slednja grupa definirana induktivno in torej v splošnem *ni* nujno kar enaka grupi, generirani s komutatorji uteži 3 oblike $[h,k,l]$ za $h \in H, k \in K, l \in L$.

Lema. Naj bosta $H,K \trianglelefteq G$, $H = \langle X \rangle$, $K = \langle Y \rangle$. Tedaj je

$$[H,K] = \langle\langle [x,y] \mid x \in X, y \in Y \rangle\rangle.$$

Dokaz. Grupa $[H,K]$ vsebuje vse komutatorje $[x,y]$ za $x \in X, y \in Y$, zato vsebuje tudi podgrupo edinko, generirano s temi elementi: $N := \langle\langle [x,y] \mid x \in X, y \in Y \rangle\rangle$. Velja tudi obratna inkluzija. V kvocientu $[H,K]/N$ namreč odsek xN komutira z yN za $x \in X, y \in Y$, zato v tem kvocientu celotna podgrupa HN/N komutira s podgrupo KN/N. Od tod sledi $[H,K]N = N$, torej je res tudi $[H,K] \leq N$. □

[5] V grupi imamo dve konjugiranji: levo in desno. Levo konjugiranje z x je $g \mapsto xgx^{-1} = {}^x g$ in to je levo delovanje, desno konjugiranje z x pa je $g \mapsto x^{-1}gx = g^x$ in to je desno delovanje.

[6] To je analog Jacobijeve identitete iz Liejevih algeber.

Komutatorji in spodnja centralna vrsta

Spodnja centralna vrsta je vselej generirana s komutatorji ustreznih uteži.

Lema. V vsaki grupi G velja $\gamma_i(G) = \langle [x_1, x_2, \ldots, x_i] \mid x_1, x_2, \ldots, x_i \in G \rangle$.

Dokaz. Indukcija na i.

- $i = 1$: ✓
- $i - 1 \to i$: Velja $\gamma_i(G) = [\gamma_{i-1}(G), G]$, zato iz zadnje leme in indukcije sledi
$$\gamma_i(G) = \langle\langle [x_1, x_2, \ldots, x_{i-1}, x_i] \mid x_1, \ldots, x_i \in G \rangle\rangle.$$
Konjugat komutatorja uteži i je komutator uteži i, velja namreč $[x_1, \ldots, x_i]^g = [x_1^g, \ldots, x_i^g]$ za $g \in G$. Tako je podgrupa, generirana s komutatorji uteži i, edinka v G. S tem je dokaz zaključen. ✓

□

V lemi *ne* smemo jemati elementov x_i le iz neke generirajoče množice $X \subseteq G$. V tem primeru namreč enak dokaz kot zgoraj pokaže, da velja

$$\gamma_i(G) = \langle\langle [x_1, \ldots, x_i] \mid x_1, \ldots, x_i \in X \rangle\rangle$$

in v splošnem podgrupa, generirana s komutatorji uteži i s členi v X *ni* nujno edinka v G.

Zgled. Opazujmo diedrsko grupo $D_{2n} = \langle s, t \mid s^n, t^2, tst^{-1} = s^{-1} \rangle$. Vzemimo $X = \{s, t\}$. Izračunamo

$$\gamma_2(D_{2n}) = \langle\langle [s, t] \rangle\rangle = \langle\langle s^2 \rangle\rangle = \langle s^2 \rangle.$$

Za tem je

$$\gamma_3(D_{2n}) = [\gamma_2(D_{2n}), G] = \langle\langle [s^2, t] \rangle\rangle = \langle\langle s^4 \rangle\rangle = \langle s^4 \rangle$$

in nato

$$\gamma_4(D_{2n}) = [\gamma_3(D_{2n}), G] = \langle\langle [s^4, t] \rangle\rangle = \langle s^8 \rangle.$$

Induktivno velja $\gamma_i(D_{2n}) = \langle s^{2^{i-1}} \rangle$ za $i \geq 2$.

Naj bo $n = 2^a m$ za $a, m \in \mathbb{N}_0$, pri čemer je m liho število. Velja $\gamma_{a+1}(D_{2n}) = \langle s^{2^a} \rangle = \langle s^{n/m} \rangle$. Če je $m = 1$, potem sledi $\gamma_{a+1}(D_{2n}) = 1$, torej je v tem primeru grupa D_{2n} nilpotentna razreda a. Če pa je $m > 1$, potem je $s^{n/m}$ lihega reda m, zato je $\gamma_i(D_{2n}) = \langle s^{n/m} \rangle$ za vsak $i \geq a + 1$. V tem primeru grupa D_{2n} torej *ni* nilpotentna.

Podobno velja v primeru $n = \infty$. Spodnja centralna vrsta nikdar ne doseže 1 in grupa D_∞ *ni* nilpotentna.

V kvocientu $G/\gamma_i(G)$ so vsi komutatorji uteži i trivialni, zato so vsi komutatorji uteži $i - 1$ centralni. Torej je edinka, generirana s komutatorji uteži $i - 1$, enaka podgrupi, generirani s komutatorji uteži $i - 1$. Skupaj z zgornjo opombo od tod sledi naslednja posledica.

Posledica. Naj bo $G = \langle X \rangle$. Grupa $\gamma_{i-1}(G)/\gamma_i(G)$ je generirana s komutatorji uteži $i - 1$ z vnosi iz množice $X\gamma_i(G)/\gamma_i(G)$.

Kadar je grupa G končno generirana, so torej kvocienti spodnje centralne vrste končno generirane abelove grupe. V posebnem zato velja naslednje.

Posledica. Končno generirana nilpotentna grupa je policiklična.

Končno generirana torzijska[7] nilpotentna grupa je torej policiklična z verigo brez neskončnih kvocientov, torej je taka grupa nujno končna. Velja pa še nekaj močnejšega.

Trditev. Naj bo G *nilpotentna* grupa, generirana s končno mnogo torzijskimi elementi. Tedaj je G končna.

Dokaz. Dokažimo, da je za vsak i grupa $\gamma_i(G)/\gamma_{i+1}(G)$ končna. Od tod bo sledilo, da je tudi G končna. Naj bo $G = \langle X \rangle$ z lastnostjo $x^N = 1$ za vse $x \in X$. Grupa $\gamma_i(G)/\gamma_{i+1}(G)$ je generirana s komutatorji uteži i z vnosi iz množice $X\gamma_{i+1}(G)/\gamma_{i+1}(G)$. Za vsak tak komutator $[x_1,\ldots,x_i]\gamma_{i+1}$ velja

$$([x_1,\ldots,x_i]\gamma_{i+1})^N = [x_1,\ldots,x_{i-1},x_i^N]\gamma_{i+1}(G) = \gamma_{i+1}(G),$$

kjer smo v prvi enakosti uporabili drugo komutatorsko identiteto. Tako je abelova grupa $\gamma_i(G)/\gamma_{i+1}(G)$ generirana s končno mnogo elementi reda kvečjemu N, torej je končna. □

Zgled. Grupa D_∞ je generirana s torzijskima elementoma t, st, a ta grupa ni končna.

Odprt problem. (Burnside 1902) Ali je grupa

$$B(2,5) = \langle x, y \mid w^5 = 1 \text{ za vsako besedo } w \in F(\{x,y\}) \rangle$$

končna?

3.3 Teorija razširitev

Problem rekonstrukcije

Naj bo G končna grupa. Če G *ni* enostavna, potem ima pravo netrivalno edinko N. Torej lahko G predstavimo kot razširitev:

$$1 \to N \to G \to G/N \to 1.$$

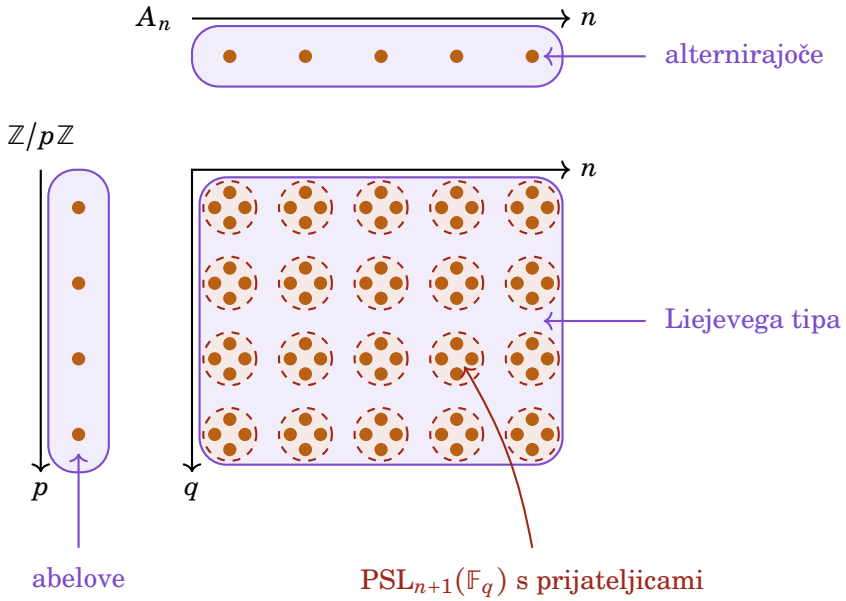
Ta postopek lahko nadaljujemo z grupama N in G/N. Torej lahko grupo G dobimo z zaporednim izvajanjem razširitev: začnemo z enostavno grupo G/N_1, ki jo razširimo z enostavno grupo N_1/N_2, tako dobimo grupo G/N_2, ki jo potem razširimo z enostavno grupo N_2/N_3, tako dobimo grupo G/N_3, $\ldots$, nazadnje dobimo grupo $G/N_k = G$.

V prejšnjem razdelku smo obravnavali policiklične grupe – to so natanko grupe, pri katerih so vsi kvocienti N_i/N_{i+1} v zgornji konstrukciji ciklični.

V tem razdelku si bomo podrobneje pogledali, do kakšne mere lahko s poznavanjem teh enostavnih kvocientov *rekonstruiramo* grupo G.

Kakšne možnosti imamo za enostavne kose? Katere so vse končne enostavne grupe? Končne enostavne grupe so klasificirane (res?), sestojijo iz naslednjih družin:

[7] Grupa je torzijska, če je vsak njen element končnega reda.



Slika 3.1: Prikaz klasifikacije končnih enostavnih grup

- ciklične grupe: $\mathbb{Z}/p\mathbb{Z}$,
- alternirajoče grupe: A_n za $n \geq 5$,
- matrične grupe Liejevega tipa: $\mathrm{PSL}_{n+1}(\mathbb{F}_q)$ za $n \geq 1$, kjer je q potenca praštevila in $\mathbb{F}_q$ končno polje moči q; sorodne tej so ortogonalne, simplektične in unitarne grupe,
- izjemne grupe Liejevega tipa: te so uresničljive kot podgrupe matrik majhnih dimenzij,
- končno mnogo sporadičnih grup.

Mi bomo obravnavali le *najlažji primer*, ko predpostavimo, da so vsi enostavni kosi kar ciklične grupe. S tem primerom pokrijemo vse končne rešljive grupe, hkrati pa je že ta primer zelo zakompliciran, kot bomo videli.

Kategorija razširitev

Množica vseh razširitev tvori *kategorijo*. Njeni objekti so razširitve, morfizem med razširitvama $N \xrightarrow{\iota} G \xrightarrow{\pi} Q$ in $\bar{N} \xrightarrow{\bar{\iota}} \bar{G} \xrightarrow{\bar{\pi}} \bar{Q}$ je trojica homomorfizmov (α, β, γ), tako da naslednji diagram komutira:

$$\begin{array}{ccccc} N & \xrightarrow{\iota} & G & \xrightarrow{\pi} & Q \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ \bar{N} & \xrightarrow{\bar{\iota}} & \bar{G} & \xrightarrow{\bar{\pi}} & \bar{Q}. \end{array}$$

Morfizem, pri katerem je $\alpha = \mathrm{id}_N$ in $\gamma = \mathrm{id}_Q$ (in torej $N = \bar{N}$, $Q = \bar{Q}$), imenujemo ekvivalenca razširitev. V tem primeru je β nujno izomorfizem grup G in $\bar{G}$ (→ vaje).

Delovanje v razširitvi z abelovim jedrom

Predpostavimo, da je N *abelova* grupa. V tem primeru je kategorija vseh razširitev *blage zahtevnosti* in jo lahko opišemo na naslednji način.

Naj bo $N \xrightarrow{\iota} G \xrightarrow{\pi} Q$ objekt kategorije razširitev. Izberimo transverzalo $\mathcal{T}$: za vsak odsek N v G izberemo en element iz tega odseka. Elementi $\mathcal{T}$ so torej v bijekciji z elementi Q prek preslikave π. Ekvivalentno, imamo prerezno funkcijo[8] $\tau: Q \to G$, za katero za vsak $q \in Q$ velja $\tau(q) \in \mathcal{T}$ in $\pi(\tau(q)) = q$.

Vemo že, da v primeru, ko lahko izberemo prerezno funkcijo tako, da je homomorfizem, dobimo semidirektni produkt. Kaj pa v primeru, ko τ ni nujno homomorfizem?

Elementi transverzale $\mathcal{T}$ delujejo na N s konjugiranjem: za $n \in N$ dobimo ${}^{\tau(q)}n = \tau(q) \cdot n \cdot \tau(q)^{-1}$. Na ta način dobimo *homomorfizem*[9] $\chi: Q \to \mathrm{Aut}(N)$, ki q preslika v konjugiranje s $\tau(q)$. Torej dobimo delovanje Q na N. To delovanje je *neodvisno od izbire transverzale* $\mathcal{T}$ oziroma prerezne funkcije τ (→ vaje).

Povzemimo.

Trditev. Vsaka razširitev $N \xrightarrow{\iota} G \xrightarrow{\pi} Q$ z abelovim jedrom N porodi homomorfizem $\chi: Q \to \mathrm{Aut}(N)$.

Zgled. Naj bo $G = N \rtimes_\varphi Q$, kjer je $\varphi: Q \to \mathrm{Aut}(N)$. Tedaj lahko izberemo transverzalo s prerezno funkcijo $\tau: Q \to G, q \mapsto (1, q)$. Velja

$$ {}^{\tau(q)}n = {}^{(1,q)}(n,1) = (1,q)(n,1)(1,q)^{-1} = (\varphi(q)(n),1) = \varphi(q)(n). $$

Torej je $\chi(q) = \varphi(q)$ za vsak $q \in Q$, se pravi $\chi = \varphi$.

Kako se χ spremeni z ekvivalenco razširitev?

Trditev. Ekvivalentni razširitvi z abelovim jedrom porodita enak homomorfizem $\chi: Q \to \mathrm{Aut}(N)$.

Dokaz. Imejmo ekvivalentni razširitvi $N \xrightarrow{\iota} G \xrightarrow{\pi} Q$ in $N \xrightarrow{\bar{\iota}} \bar{G} \xrightarrow{\bar{\pi}} Q$ z izomorfizmom $\beta: G \to \bar{G}$ in s pripadajočima delovanjema $\chi, \bar{\chi}: Q \to \mathrm{Aut}(N)$. Izberimo prerezno funkcijo $\tau: Q \to G$ za π. Tedaj je $\beta \circ \tau: Q \to \bar{G}$ prerezna funkcija za $\bar{\pi}$. Za $n \in N$ in $q \in Q$ velja

$$ \chi(q)(n) = {}^{\tau(q)}n $$

in

$$ \bar{\chi}(q)(n) = {}^{\beta(\tau(q))}n = \beta(\tau(q))n\beta(\tau(q))^{-1}. $$

Ker je $\beta|_N = \mathrm{id}_N$, je zadnji element enak

$$ \beta(\tau(q))\beta(n)\beta(\tau(q))^{-1} = \beta({}^{\tau(q)}n) = \beta(\chi(q)(n)) = \chi(q)(n). $$

Tako je res $\chi = \bar{\chi}$. □

Ni pa vsa informacija o razširitvi skrita v homomorfizmu χ. Lahko se zgodi, da imata dve neekvivalentni razširitvi enak χ.

[8] Prerezna funkcija v splošnem ni nujno homomorfizem.

[9] Za $q_1, q_2 \in Q$ velja $\tau(q_1q_2) \equiv \tau(q_1)\tau(q_2) \mod N$. Ker je N *abelova*, je torej konjugiranje z $\tau(q_1q_2)$ enako konjugiranju z $\tau(q_1)\tau(q_2)$. Zato je χ res homomorfizem.

Zgled. Opazujmo dve razširitvi grupe $\mathbb{Z}/2\mathbb{Z}$ z $\mathbb{Z}/2\mathbb{Z}$. Prva naj bo kar trivialna razširitev, kjer je srednja grupa enaka $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Druga naj bo razširitev, kjer je srednja grupa enaka $\mathbb{Z}/4\mathbb{Z}$. Ti dve razširitvi sta jasno neekvivalentni. Delovanji v obeh primerih slikata iz $\mathbb{Z}/2\mathbb{Z}$ v grupo $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z})$. Slednja grupa je trivialna in vsebuje le $\mathrm{id}_{\mathbb{Z}/2\mathbb{Z}}$. V vsakem primeru sta torej pripadajoči delovanji trivialni, torej enaki.

Kohomologija

Ključ v razumevanju razširitve je v tem, da pogledamo, kako *daleč* je prerezna funkcija τ od homomorfizma.

Naj bo $N \xrightarrow{\iota} G \xrightarrow{\pi} Q$ razširitev z izbrano prerezno funkcijo τ. Ker za vsak $q_1, q_2 \in Q$ velja $\tau(q_1q_2) \equiv \tau(q_1)\tau(q_2) \mod N$, obstaja enoličen $n = n(q_1,q_2) \in N$, za katerega je $n\cdot\tau(q_1q_2) = \tau(q_1)\tau(q_2)$. Dobimo torej funkcijo

$$\phi\colon Q\times Q \to N, \quad (q_1,q_2)\mapsto n(q_1,q_2).$$

Ta funkcija ni čisto poljubna. Iz asociativnosti množenja namreč izpeljemo naslednji račun: po eni strani je za poljubne $q_1,q_2,q_3\in Q$ produkt $\tau(q_1)\tau(q_2)\tau(q_3)$ enak

$$\begin{aligned}(\tau(q_1)\tau(q_2))\tau(q_3) &= \phi(q_1,q_2)\tau(q_1q_2)\tau(q_3)\\ &= \phi(q_1,q_2)\phi(q_1q_2,q_3)\tau(q_1q_2q_3),\end{aligned}$$

po drugi strani pa je enak

$$\begin{aligned}\tau(q_1)(\tau(q_2)\tau(q_3)) &= \tau(q_1)\phi(q_2,q_3)\tau(q_2q_3)\\ &=^{\tau(q_1)} \phi(q_2,q_3)\cdot\tau(q_1)\tau(q_2q_3)\\ &= q_1.\phi(q_2,q_3)\cdot\phi(q_1,q_2q_3)\tau(q_1q_2q_3),\end{aligned}$$

kjer Q deluje na N prek homomorfizma χ. Na ta način dobimo naslednji pogoj, ki mu zadošča funkcija ϕ:

$$\forall q_1,q_2,q_3\in Q\colon \quad \phi(q_1,q_2)+\phi(q_1q_2,q_3) = q_1.\phi(q_2,q_3)+\phi(q_1,q_2q_3)$$

Tukaj smo operacijo v N zaradi preglednosti pisali aditivno. Vsaki funkciji $\phi\colon Q\times Q\to N$, ki zadošča temu nenavadnemu pogoju, rečemo 2-kocikel. Množico vseh 2-kociklov označimo z $Z^2(Q,N)$.

> Razširitvi smo torej z nekaj izbire priredili prerezno preslikavo τ, tej pa zdaj še 2-kocikel ϕ.

V množici $Z^2(Q,N)$ lahko seštevamo z uporabo operacije na N: za 2-kocikla $\phi_1,\phi_2\colon Q\times Q\to N$ je $(\phi_1+\phi_2)(q_1,q_2) = \phi_1(q_1,q_2)+\phi_2(q_1,q_2)$ za $q_1,q_2\in N$. Na ta način je $Z^2(Q,N)$ abelova grupa.

Zgled. Če je $G = N\rtimes_\varphi Q$, potem je τ homomorfizem, zato dobimo $\phi\equiv 0$.

Kako je ϕ odvisen od izbire τ? Naj bo τ' še en prerez π. Tako dobimo drug 2-kocikel $\phi'\in Z^2(Q,N)$. Velja $\tau(q)\equiv\tau'(q) \mod N$, zato obstaja enoličen $n = n(q)\in N$, za katerega je $n\cdot\tau'(q) = \tau(q)$. Dobimo torej funkcijo

$$\psi\colon Q\to N, \quad q\mapsto n(q).$$

Funkciji ϕ in ϕ' sta povezani prek funkcije ψ na naslednji način. Za $q_1, q_2 \in Q$ velja

$$\begin{aligned}\phi(q_1,q_2) &= \tau(q_1)\cdot\tau(q_2)\cdot\tau(q_1q_2)^{-1}\\ &= \psi(q_1)\tau'(q_1)\cdot\psi(q_2)\tau'(q_2)\cdot\tau'(q_1q_2)^{-1}\psi(q_1q_2)^{-1}\\ &= \psi(q_1)\cdot{}^{\tau'(q_1)}\psi(q_2)\cdot\tau'(q_1)\tau'(q_2)\tau'(q_1q_2)^{-1}\cdot\psi(q_1q_2)^{-1}\\ &= \psi(q_1)+q_1.\psi(q_2)+\phi'(q_1,q_2)-\psi(q_1q_2),\end{aligned}$$

kjer smo v zadnji vrstici operacijo v N pisali aditivno. Definirajmo funkcijo

$$\psi^\star : Q\times Q \to N, \quad (q_1,q_2)\mapsto \psi(q_1)+q_1.\psi(q_2)-\psi(q_1q_2).$$

Na ta način po zgornjem računu velja $\phi = \phi' + \psi^\star$. Ker sta ϕ, ϕ' elementa grupe $Z^2(Q,N)$, je tudi $\psi^\star = \phi - \phi' \in Z^2(Q,N)$.

Naj bo $B^2(Q,N)$ množica vseh funkcij $f^\star : Q\times Q \to N$, za katere obstaja funkcija $f : Q \to N$, tako da velja $f^\star(q_1,q_2) = f(q_1) + q_1.f(q_2) - f(q_1q_2)$. Elementom te množice rečemo 2-korobovi. Ni težko (je pa sitno) preveriti, da je $B^2(Q,N)$ podgrupa grupe $Z^2(Q,N)$.

Iz zgodnje izpeljave sledi, da je funkcija $\psi^\star = \phi - \phi'$ 2-korob.

> Razširitvi smo torej z izbiro prereza τ priredili 2-kocikel ϕ, z izbiro drugega prereza τ' 2-kocikel ϕ', ta dva kocikla pa se razlikujeta za 2-korob $\psi^\star$.

Če identificiramo 2-kocikle, ki se razlikujejo za 2-korob, je torej dobljen ekvivalenčni razred 2-kocikla neodvisen od izbire prerezne funkcije. Povzemimo.

Trditev. Razširitev $N \to G \to Q$ z abelovim jedrom N porodi element $\phi + B^2(Q,N)$ grupe $Z^2(Q,N)/B^2(Q,N)$.

Grupo $Z^2(Q,N)/B^2(Q,N)$ označimo s $H^2(Q,N)$ in ji pravimo druga kohomološka grupa, prirejena delovanju grupe Q na N. Za njeno definicijo potrebujemo le grupi Q in N ter delovanje $\chi : Q \to \mathrm{Aut}(N)$.

> Razširitvi smo torej enolično priredili kohomološki element $\phi + B^2(Q,N)$. Ali vsak kohomološki element izhaja iz neke razširitve?

Naj bo $\phi \in Z^2(Q,N)$ dan 2-kocikel. Iz njega lahko sestavimo razširitev na naslednji način. Naj bo grupa $G(\phi)$ kot množica enaka $N\times Q$, množenje na njej pa vpeljemo z naslednjim predpisom:

$$(n_1,q_1)\cdot(n_2,q_2) = (n_1 + q_1.n_2 + \phi(q_1,q_2), q_1q_2)$$

za $n_1, n_2 \in N$, $q_1, q_2 \in Q$. Pri tem smo operacijo na N zopet pisali aditivno. S tem predpisom je $G(\phi)$ grupa. Opremljena je tudi z naravnima preslikavama $\iota : N \to G(\phi), n \mapsto (n,1)$ in $\pi : G(\phi) \to Q, (n,q) \mapsto q$. Kateri kohomološki element ustreza razširitvi $N \xrightarrow{\iota} G(\phi) \xrightarrow{\pi} Q$?

Trditev. Naj bo $\chi : Q \to \mathrm{Aut}(N)$ delovanje na abelovi grupi N in naj bo $\phi \in Z^2(Q,N)$. Razširitev $N \xrightarrow{\iota} G(\phi) \xrightarrow{\pi} Q$ porodi ravno delovanje χ na N, hkrati pa *obstaja* prerezna funkcija $\tau : Q \to G(\phi)$, da je 2-kocikel te razširitve ravno ϕ.

Dokaz. Za τ lahko vzamemo funkcijo $q \mapsto (1,q)$ za $q \in Q$. □

> Razširitvi smo torej enolično priredili kohomološki element. To prirejanje ima *prerezno* prirejanje razširitve 2-kociklu. Kako je razširitev $G(\phi)$ odvisna od izbire 2-kocikla ϕ v kohomološki grupi?

Naj bosta $\phi, \phi' \in Z^2(Q,N)$, ki se razlikujeta za 2-korob $\psi^\star \in B^2(Q,N)$, ki sam izhaja iz preslikave $\psi: Q \to N$. Priredimo jima razširitvi $G(\phi), G(\phi')$. Definirajmo preslikavo

$$\beta: G(\phi) \to G(\phi'), \quad (n,q) \mapsto (n + \psi(q), q).$$

Ni težko preveriti, da β vzpostavi ekvivalenco razširitev $N \to G(\phi) \to Q$ in $N \to G(\phi') \to Q$.

Velja tudi obratno. Imejmo ekvivalentni razširitvi $N \xrightarrow{\iota} G \xrightarrow{\pi} Q$ in $N \xrightarrow{\bar{\iota}} \bar{G} \xrightarrow{\bar{\pi}} Q$ z izomorfizmom $\beta: G \to \bar{G}$. Izberimo prerezno funkcijo τ prve razširitve. Tedaj je $\bar{\tau} = \beta \circ \tau$ prerezna funkcija druge razširitve. Naj bo $\phi \in Z^2(Q,N)$ prirejen prerezni funkciji τ. Tedaj za $q_1, q_2 \in Q$ velja

$$\tau(q_1)\tau(q_2) = \phi(q_1,q_2)\tau(q_1 q_2),$$

od koder po uporabi β sledi

$$\bar{\tau}(q_1)\bar{\tau}(q_2) = \phi(q_1,q_2)\bar{\tau}(q_1 q_2),$$

torej je ϕ ravno 2-kocikel, prirejen prerezni funkciji $\bar{\tau}$. Obe razširitvi torej porodita isti kohomološki element $\phi + B^2(Q,N) \in H^2(Q,N)$.

Tako smo nazadnje dokazali naslednji izrek.

Izrek. Naj grupa Q deluje na abelovi grupi N. Tedaj obstaja bijekcija med ekvivalenčnimi razredi razširitev Q z N z danim delovanjem in elementi kohomološke grupe $H^2(Q,N)$. Pri tem razcepna razširitev ustreza enoti kohomološke grupe.

Zgled. Naj bo $N = (\mathbb{Z}/2\mathbb{Z})^2$ in $Q = D_8$. Izberimo trivialno delovanje grupe Q na N, torej $\chi: Q \to \mathrm{Aut}(N), q \mapsto \mathrm{id}_N$. Zahteven, a trivialen račun pokaže, da velja

$$Z^2(Q,N) \cong (\mathbb{Z}/2\mathbb{Z})^8, \quad B^2(Q,N) \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Torej je $H^2(Q,N) \cong (\mathbb{Z}/2\mathbb{Z})^6$. Imamo torej $2^6 = 64$ neekvivalentnih razširitev pri trivialnem delovanju Q na N. Ni pa nujno, da vsaka dva kohomološka elementa porodita *neizomorfni* razširitveni grupi. Izkaže se, da v resnici dobimo le 11 neizomorfnih grup. Konkreten primer netrivialne razširitve je

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\iota} \mathbb{Z}/2\mathbb{Z} \times D_{16} \xrightarrow{\pi} D_8,$$

kjer je $\iota(x,y) = (x, \rho^{4y})$ in $\pi(x, \sigma^i \rho^j) = \sigma^i \rho^j$.

Če opazujemo le razširitve 2-grup z 2-grupami, dobimo naslednje število neizomorfnih grup:

i	število grup moči 2^i
1	1
2	2
3	5
4	14
5	51
6	267
7	2328
8	$\sim 5.6 \cdot 10^4$
9	$\sim 10^7$
10	$\sim 4.95 \cdot 10^{10}$

Po drugi strani je število *vseh* grup moči kvečjemu 2000 enako $\sim 4.99 \cdot 10^{10}$. Lahko bi torej rekli, da so *skoraj vse končne grupe 2-grupe*.

Odprt problem. Naj bo $A(n)$ število grup moči kvečjemu n. Naj bo $B(n)$ število 2-grup moči kvečjemu n. Tedaj je $\lim_{n\to\infty} B(n)/A(n) = 1$.

Domnevno je torej skoraj vsa kompleksnost končnih grup skrita v teoriji zaporednih razširitev z grupo $\mathbb{Z}/2\mathbb{Z}$. Pri tem je $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}) = 1$, torej je vsako delovanje na tej grupi trivialno.

Poglavje 4

Rast

4.1 Funkcija rasti

Besedna metrika

Naj bo G končno generirana grupa, $G = \langle S \rangle$. Cayleyjev graf $\mathrm{Cay}(G,S)$ je metrični prosto glede na razdaljo

$$d_S(g,h) = \min\{n \mid n \in \mathbb{N}_0,\ gs_1s_2\cdots s_n = h,\ s_i \in S \cup S^{-1}\}$$

za $g,h \in G$. Merimo torej dolžino najkrajše poti v $\mathrm{Cay}(G,S)$ med vozliščema g in h. Označimo $\ell_S(g) = d_S(g,1)$, to je dolžina elementa $g \in G$ glede na množico S.

Naj bo $B_{G,S}(r) = \{g \in G \mid \ell_S(g) \leq r\}$ krogla polmera r okoli enote 1 v $\mathrm{Cay}(G,S)$. Sorodno vpeljemo sfero $S_{G,S}(r) = \{g \in G \mid \ell_S(g) = r\}$.

Funkcija rasti

Funkcija rasti je funkcija, ki šteje število elementov v krogli oziroma sferi v odvisnosti od polmera. Natančneje imamo torej dve funkciji rasti:

$$\beta_{G,S}\colon \mathbb{N}_0 \to \mathbb{N}_0, \quad n \mapsto |B_{G,S}(n)|$$

in

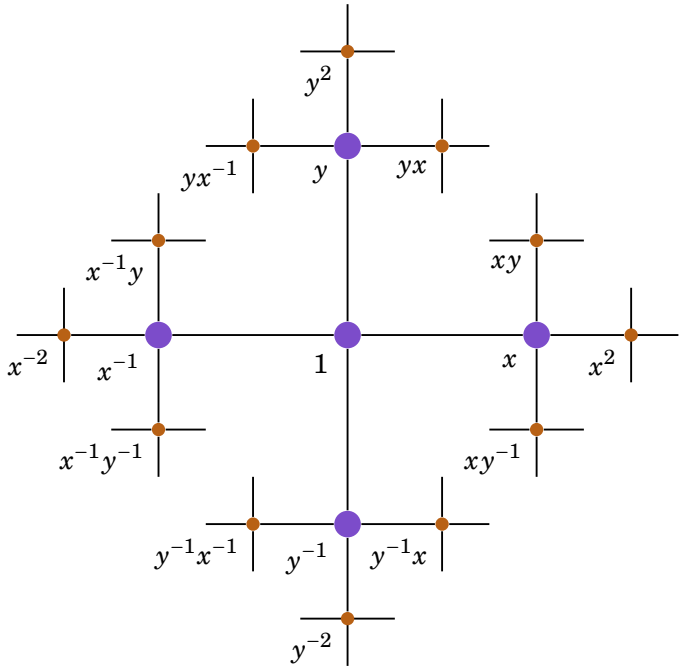
$$\sigma_{G,S}\colon \mathbb{N}_0 \to \mathbb{N}_0, \quad n \mapsto |S_{G,S}(n)|.$$

Funkciji $\beta_{G,S}$ včasih rečemo tudi kumulativna funkcija rasti. Ponavadi z izrazom funkcija rasti mislimo na slednjo funkcijo.

Zgled.

- Opazujmo grupo $\mathbb{Z} = \langle 1 \rangle$. Za celo število $a \in \mathbb{Z}$ je $\ell_{\{1\}}(a) = |a|$. Velja torej
$$\sigma_{\mathbb{Z},\{1\}}(n) = \begin{cases} 1; & n = 0 \\ 2; & n > 0 \ (\pm n) \end{cases}$$
in $\beta_{\mathbb{Z},\{1\}}(n) = 2n+1$. Slednja funkcija je linearna, zato rečemo, da imamo linearno funkcijo rasti.

- Opazujmo grupo $\mathbb{Z} = \langle 2,3 \rangle$. Vsako celo število $a \in \mathbb{Z}$ lahko zapišemo v obliki $a = 2r+3s$ za neka $r,s \in \mathbb{Z}$. Tako je $\ell_{\{2,3\}}(a) \leq |r| + |s|$. Če je $r \geq 3$, potem lahko a zapišemo tudi v obliki $a = 2(r-3)+3(s+2)$, s čimer smo skrajšali dolžino zapisa za 1. Minimalno dolžino zapisa a dobimo torej z zapisom v obliki, ki je odvisna od ostanka a pri deljenju s 3. Predpostavimo, da je $a \geq 2$.



Slika 4.1: $B_{F_2,\{x,y\}}(1)$

- *Če je* $a = 3k$ *za nek* $k \in \mathbb{Z}$*:* V tem primeru je $\ell_{\{2,3\}}(a) = k$.
- *Če je* $a = 3k+2$ *za nek* $k \in \mathbb{Z}$*:* V tem primeru je $\ell(a) = k+1$.
- *Če je* $a = 3k+1$ *za nek* $k \in \mathbb{Z}$*:* V tem primeru je $\ell(a) = k+1$, saj imamo zapis $a = 3(k-1)+2\cdot 2$.

Jasno velja tudi $\ell_{\{2,3\}}(1) = 2$ in $\ell_{\{2,3\}}(0) = 0$. Analogne dolžine dobimo za $a < 0$. Skupaj torej velja:

$$\sigma_{\mathbb{Z},\{2,3\}}(n) = \begin{cases} 1; & n = 0 \\ 4; & n = 1 \ (\pm 2, \pm 3) \\ 8; & n = 2 \ (\pm 4, \pm 6, \pm 5, \pm 1) \\ 6; & n \geq 3 \ (\pm 3n, \pm(3(n-1)+2), \pm(3(n-2)+2\cdot 2) \end{cases}$$

Domača naloga. Dokaži, da za tuji števili $r, s \in \mathbb{Z}$, $0 < r < s$, velja $\sigma_{\mathbb{Z},\{r,s\}}(n) = 2s$ za vse dovolj velike n.

Od tod izračunamo kumulativno funkcijo rasti za $n \geq 2$:

$$\beta_{\mathbb{Z},\{2,3\}}(n) = \sum_{i=0}^{n} \sigma_{\mathbb{Z},\{2,3\}}(i) = 13 + 6(n-2),$$

torej imamo zopet linearno funkcijo rasti.

- Opazujmo diedrsko grupo $D_\infty = \langle s, t \mid t^2, tst^{-1} = s^{-1} \rangle$. Vsak element $a \in D_\infty$ lahko zapišemo enolično bodisi kot $a = s^k$ bodisi kot $a = ts^k$ za nek $k \in \mathbb{Z}$. Dolžina prvega elementa je $|k|$, dolžina drugega pa $|k|+1$. Tako je

$$\sigma_{D_\infty,\{s,t\}}(n) = \begin{cases} 1; & n = 0 \\ 3; & n = 1 \ (s^{\pm 1}, t) \\ 4; & n \geq 2 \ (s^{\pm n}, ts^{\pm(n-1)}) \end{cases}$$

in za tem $\beta_{D_\infty,\{s,t\}}(n) = 4 + 4(n-2)$ za $n \geq 2$. Zopet imamo linearno funkcijo rasti.

- Opazujmo grupo $\mathbb{Z}^d$ za $d \in \mathbb{N}$, generirano s standardno bazo $e_i = (0,\dots,0,1,0,\dots,0)$ za $i = 1,2,\dots,d$. Vsak element $a \in \mathbb{Z}^d$ lahko zapišemo enolično kot $a = \sum_{i=1}^{n} \alpha_i e_i$ za neke $\alpha_i \in \mathbb{Z}$, dolžina takega elementa pa je enaka $\sum_{i=1}^{n} |\alpha_i|$. V posebnem primeru $d = 2$ tako dobimo

  $$\sigma_{\mathbb{Z}^2,\{e_1,e_2\}}(n) = |\{(\alpha_1,\alpha_2) \in \mathbb{Z}^2 \mid |\alpha_1| + |\alpha_2| = n\}|.$$

  V splošnem lahko za izračun funkcije rasti z upoštevanjem vrednosti α_d izpeljemo rekurzivno zvezo:

  $$\sigma_{\mathbb{Z}^d,\{e_1,\dots,e_d\}}(n) = \sigma_{\mathbb{Z}^{d-1},\{e_1,\dots,e_{d-1}\}}(n) + \sum_{k=1}^{n} 2 \cdot \sigma_{\mathbb{Z}^{d-1},\{e_1,\dots,e_{d-1}\}}(n-k).$$

  V posebnem primeru $d = 2$ od tod izpeljemo

  $$\sigma_{\mathbb{Z}^2,\{e_1,e_2\}}(n) = \begin{cases} 1; & n = 0 \\ 2 + \sum_{k=1}^{n-1} 2 \cdot 2 + 2 = 4n; & n > 0 \end{cases}$$

  in s tem $\beta_{\mathbb{Z}^2,\{e_1,e_2\}}(n) = 1 + \sum_{k=1}^{n} 4k = 2n^2 + 2n + 1$. Tu imamo torej kvadratno funkcijo rasti.

  Preprosta indukcija z uporabo gornje rekurzivne zveze dokaže, da je $\beta_{\mathbb{Z}^d,\{e_1,\dots,e_d\}}$ polinom stopnje d.

- Opazujmo prosto grupo F_d ranga d z generatorji $S = \{x_1^{\pm 1},\dots,x_d^{\pm 1}\}$. Njeni elementi so okrajšane besede v S. Velja torej $\sigma_{F_d,S}(n) = 2d \cdot (2d-1)^{n-1}$ za $n \geq 1$ in zato $\beta_{F_d,S}(n) = 1 + \sum_{k=1}^{n} 2d(2d-1)^{k-1} = 1 + 2d \cdot \frac{(2d-1)^n - 1}{2d-2}$. V tem primeru imamo torej eksponentno funkcijo rasti.

Ekvivalenca funkcij rasti

Za dani funkciji $f, g : \mathbb{N} \to \mathbb{R}$ uvedemo oznako

$$f \preceq g \quad \Leftrightarrow \quad \exists A \in \mathbb{R}_{>0}\ \forall n \in \mathbb{N}:\ f(n) \leq A \cdot g(An).$$

Rečemo, da sta funkciji f in g ekvivalentni, če velja $f \preceq g$ in $g \preceq f$. V tem primeru pišemo $f \sim g$.

Zgled. Funkciji $\beta_{\mathbb{Z},\{1\}}(n) = 2n + 1$ in $\beta_{\mathbb{Z},\{2,3\}}(n) = 6n + 1$ sta ekvivalentni.

V splošnem je rastna funkcija do ekvivalence natančno neodvisna od izbire generirajoče množice.

Trditev. Vsaki dve rastni funkciji iste grupe sta ekvivalentni.

Dokaz. Naj bo $G = \langle X \rangle = \langle Y \rangle$ za neki končni množici X, Y. Definirajmo

$$A = \max\{\max\{\ell_Y(x) \mid x \in X\}, \max\{\ell_X(y) \mid y \in Y\}\}.$$

Torej za $g \in G$ velja $\ell_X(g) \leq A \cdot \ell_Y(g)$ in $\ell_Y(g) \leq A \cdot \ell_X(g)$. Od tod sledi $\sigma_{G,Y}(n) \leq \sigma_{G,X}(An)$ in $\sigma_{G,X}(n) \leq \sigma_{G,Y}(An)$, torej je $\sigma_{G,Y} \sim \sigma_{G,X}$. Enako velja za $\beta_{G,X}$, $\beta_{G,Y}$. □

Torej je rast *odvisna le od grupe*, če jo obravnavamo do ekvivalence rasti natančno. V taki situaciji bomo rastno funkcijo grupe G označili kar z β_G.

Zgled. Rastna funkcija proste grupe F_d ranga $d \geq 2$ je do ekvivalence natančno enaka

$$\beta_{F_d}(n) \sim 1 + 2d \cdot \frac{(2d-1)^n - 1}{2d-2} \sim \frac{d}{d-1} \cdot (2d-1)^n = \frac{d}{d-1} \cdot e^{n \log(2d-1)} \sim e^n.$$

Funkcija β_{F_d} je zato ekvivalentna funkciji β_{F_2}, ni pa ekvivalentna funkciji $\beta_{\mathbb{Z}}$. Vse nekomutativne proste grupe imajo torej ekvivalentno rast.

4.2 Izračun rasti

Iz zgledov v zadnjem razdelku bi se lahko zdelo, da je izračun funkcije rasti zelo preprosta reč – a temu ni tako! Kot bomo videli v tem razdelku, je izračun funkcije rasti tesno povezan z rešljivostjo besednega problema.

Izračunljivost

Rečemo, da je funkcija $f: A \to \mathbb{N}$ izračunljiva, če obstaja računalniški algoritem,[1] ki ob vnosu $a \in A$ vrne vrednost $f(a)$.

Zgled. Besedni problem končno prezentirane grupe $G = \langle S \mid R \rangle$ je rešljiv, če in samo če je karakteristična funkcija

$$c: (S \cup S^{-1})^* \to \{0,1\}, \quad s \mapsto \begin{cases} 0; & s = 1 \text{ v } G \\ 1; & s \neq 1 \text{ v } G \end{cases}$$

izračunljiva.

Izračunljivost rasti

Trditev. Bodi $G = \langle S \mid R \rangle$ končno prezentirana grupa. Besedni problem v G je rešljiv, če in samo če je njena funkcija rasti izračunljiva.

Dokaz. ($\Rightarrow$): Število $\beta_{G,S}(n)$ izračunamo tako, da naštejemo vse besede dolžine kvečjemu n s črkami $S \cup S^{-1}$ in z danim algoritmom za reševanje besednega problema preverimo, katere med njimi so enake. ✓✓

($\Leftarrow$): Grupo G predstavimo kot $G = F(S)/\langle\langle R \rangle\rangle$. Elementi grupe $\langle\langle R \rangle\rangle$ so produkti konjugatov relacij v R in njihovih inverzov. Teh elementov je števno mnogo in jih lahko uredimo v vrsto. Ko beremo to vrsto, torej naštevamo ravno vse besede v $F(S)$, ki so trivialne v G.

Opazujmo besedo $w \in (S \cup S^{-1})^*$. Ločimo dva primera.

- *Če je $w = 1$ v G:* V tem primeru bomo z naštevanjem elementov $\langle\langle R \rangle\rangle$ slej kot prej v seznamu naleteli na w in s tem dobili zagotovilo, da je res $w = 1$ v G.

[1] S pojmom računalniški algoritem natančneje mislimo na Turingov stroj.

- *Če je $w \neq 1$ v G:* V tem primeru se beseda w nikdar ne pojavi v vrsti $\langle\langle R \rangle\rangle$. Z naštevanjem elementov vrste se torej ne bomo mogli v končnem času[2] odločiti, ali je $w \neq 1$.

Če je $w = 1$ v G, potem je torej postopek naštevanja besed iz $\langle\langle R \rangle\rangle$ algoritem, ki ugotovi, da je res $w = 1$ v G. Če je $w \neq 1$, pa ta postopek ne deluje dobro in ga moramo še malo prilagoditi. Za to uporabimo izračunljivo funkcijo rasti $\beta_{G,S}$.

Naj bo n dolžina besede $w \in (S \cup S^{-1})^*$. Najprej sestavimo množico $\mathcal{B}$ vseh besed dolžine kvečjemu n v $S \cup S^{-1}$. Po tem začnemo postopek naštevanja elementov $\langle\langle R \rangle\rangle$. Če sta kakšna dva elementa x, y množice $\mathcal{B}$ enaka, potem bomo to opazili z naštevanjem elementov $\langle\langle R \rangle\rangle$, saj bomo slej kot prej naleteli na element xy^{-1}. Torej bomo z naštevanjem eleemntov $\langle\langle R \rangle\rangle$ slej kot prej (v končnem času) identificirali dovolj elementov množice $\mathcal{B}$, da nam bo ostalo natanko $\beta_{G,S}(n)$ besed, ki so vse različne v G. Po tem z naštevanjem dodatnih elementov $\langle\langle R \rangle\rangle$ ne bomo več našli nobene enakosti med besedami, saj bi sicer dobili manj kot $\beta_{G,S}(n)$ elementov dolžine kvečjemu n v G. Na tej točki zato pogledamo, kaj se je pri postopku zgodilo z besedo $w \in \mathcal{B}$. Če smo kadarkoli tekom postopka identificirali w s trivialno besedo, potem je seveda $w = 1$ v G. Če pa do te zadnje točke besede w nismo identificirali s trivialno besedo 1, potem imamo zagotovilo, da velja $w \neq 1$ v G. □

Ker obstajajo končno prezentirane grupe z nerešljivim besednim problemom, obstajajo torej tudi grupe, katerih funkcija rasti *ni* izračunljiva.

4.3 Osnovne lastnosti rasti

Tipi rasti

Naj bo G grupa in S neka njena generirajoča podmnožica. Če staknemo besedi dolžine n in m v G, dobimo besedo dolžine kvečjemu $n+m$. Obratno, vsako besedo dolžine $n+m$ lahko zapišemo kot konkatenacijo besed dolžine n in m. Velja torej

$$\sigma_{G,S}(n+m) \leq \sigma_{G,S}(n) \cdot \sigma_{G,S}(m) \quad \beta_{G,S}(n+m) \leq \beta_{G,S}(n) \cdot \beta_{G,S}(m).$$

Zaporedji $\{\sigma_{G,S}(n)\}_{n\in\mathbb{N}}$, $\{\beta_{G,S}(n)\}_{n\in\mathbb{N}}$ sta torej submultiplikativni. Prirejeni logaritmični zaporedji $\{\log \sigma_{G,S}(n)\}_{n\in\mathbb{N}}$, $\{\log \beta_{G,S}(n)\}_{n\in\mathbb{N}}$ sta zato subaditivni. Za taka zaporedja velja naslednja lastnost.

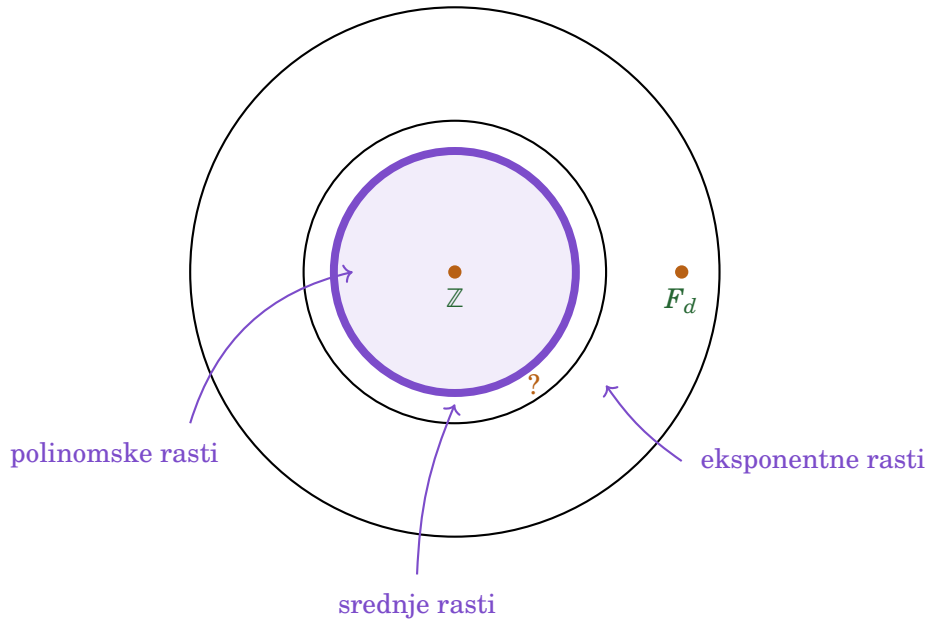
Lema. (FEKETEJEV LEMA) Naj bo $\{x_n\}_{n\in\mathbb{N}}$ nenegativno subaditivno zaporedje realnih števil. Tedaj obstaja limita $\lim_{n\to\infty} x_n/n$.

Dokaz je elementaren (→ vaje). Iz leme sledi, da obstaja limita

$$\omega_S(G) = \lim_{n\to\infty} \sqrt[n]{\sigma_{G,S}(n)} < \infty.$$

Če dodatno predpostavimo, da je grupa G neskončna, potem za vsak n velja $\sigma_{G,S}(n) \geq 1$, zato je $\omega_S(G) \geq 1$.

[2] Če $w \neq 1$, potem sicer besede res ne bomo našli v vrsti, a bomo za zagotovilo, da se to ne zgodi, morali pregledati celotno neskončno vrsto.



Slika 4.2: Diagram grup polinomske, srednje in eksponentne rasti

Lema. Velja $\lim_{n\to\infty} \sqrt[n]{\beta_{G,S}(n)} = \omega_S(G)$.

Dokaz. Označimo limito v lemi z L. Ker je $\beta_{G,S}(n) \geq \sigma_{G,S}(n)$, je jasno $L \geq \omega_S(G)$. Za obratno neenakost izberimo poljuben $\epsilon > 0$. Tedaj velja $\sigma_{G,S}(n) \leq (\omega_S(G)+\epsilon)^n$ za vse dovolj velike n, od koder sledi $\beta_{G,S}(n) \leq C + n\cdot(\omega_S(G)+\varepsilon)^n$ za neko konstanto C in za vse $n \in \mathbb{N}$. Tako dobimo $L \leq \omega_S(G)+\varepsilon$. Ker je bil ε poljuben, je dokaz zaključen. □

Zgled.

- Velja $\sigma_{\mathbb{Z},\{1\}}(n) = 2$ za vse dovolj velike n. Zato je $\omega_{\{1\}}(\mathbb{Z}) = 1$. Podobno je $\omega_{\{2,3\}}(\mathbb{Z}) = 1$.
- Velja $\sigma_{F_d,S}(n) = 2d\cdot(2d-1)^{n-1}$ za standardno generirajočo množico proste grupe S. Zato je $\omega_S(F_d) = 2d-1$.

Rečemo, da je grupa $G = \langle S\rangle$ eksponentne rasti, če je $\omega_S(G) > 1$. Kadar je $\omega_S(G) = 1$, je grupa podeksponentne rasti. Kadar velja celo $\beta_{G,S}(n) \leq C\cdot n^s$ za neki konstanti c, s in vse $n \in \mathbb{N}$, pa rečemo, da je grupa polinomske rasti. V tem zadnjem primeru definiramo še njeno stopnjo rasti kot

$$\deg_S(G) = \limsup_{n\to\infty} \frac{\log \beta_{G,S}(n)}{\log n}.$$

Grupe, katerih rast ni niti eksponentna niti polinomska, so srednje rasti.

Zgled. Grupa $\mathbb{Z} = \langle 1\rangle = \langle 2,3\rangle$ je polinomske rasti. Grupa F_d s standardno množico generatorjev je za $d \geq 2$ eksponentne rasti. Kaj pa grupe srednje rasti? Ali sploh obstajajo?

Ker sta vsaki dve rastni funkciji dane grupe ekvivalentni, sledi naslednja trditev.

Trditev. Tip rasti grupe (eksponentna, podeksponentna, polinomska, srednja) je neodvisen od izbire generatorjev. V primeru polinomske rasti je tudi stopnja rasti neodvisna od izbire generatorjev.

Od zdaj naprej bomo zato v primeru polinomske rasti namesto $\deg_S(G)$ pisali kar $\deg(G)$.

V splošnem sama vrednost $\omega_S(G)$ *ni* neodvisna od izbire generatorjev. Označimo

$$\Omega(G) = \inf_{S \subseteq G,\ \langle S\rangle = G} \omega_S(G).$$

Če za grupo G velja $\Omega(G) > 1$, potem rečemo, da je G enakomerno eksponentne rasti.

Zgled. Opazujmo prosto grupo F_2. Premislimo, da velja $\Omega(F_2) \geq 3$, torej je F_2 enakomerno eksponentne rasti. V ta namen naj bo $F_2 = \langle S\rangle$ za neko končno podmnožico $S \subseteq F_2$. V S izberimo dva elementa, ki ne komutirata, recimo jima x, y. Ta dva elementa zato generirata prosto podgrupo $H = \langle x, y\rangle \leq F_2$. Tako velja $\beta_{F_2,S}(n) \geq \beta_{H,\{x,y\}}(n) = 4 \cdot 3^{n-1}$. Od tod sledi $\omega_S(F_2) \geq 3$. Torej je res $\Omega(F_2) \geq 3$.

Ni težko premisliti (→ vaje), da za prosto grupo F_d ranga d velja celo $\Omega(F_d) = 2d - 1$.

Rast in podgrupe ter kvocienti

Pri jemanju podgrup in kvocientov dane grupe se rastni tip ne *poveča*.

Trditev. Naj bosta G, H končno generirani grupi, $H \leq G$, in naj bo $N \trianglelefteq G$. Če je G polinomske ali podeksponentne rasti, sta taki tudi H in G/N. V primeru polinomske rasti rasti velja $\deg(H), \deg(G/N) \leq \deg(G)$.

Dokaz. Naj bo $G = \langle S\rangle, H = \langle T\rangle$. Naj bo $C = \max\{\ell_S(t) \mid t \in T\}$. Tedaj je $\beta_{H,T}(n) \leq \beta_{G,S}(Cn)$. Očitno je tudi $\beta_{G/N,SN/N}(n) \leq \beta_{G,S}(n)$. Trditev sledi. □

Zgled. Opazujmo prosto grupo $F_2 = \langle x, y\rangle$. Ta vsebuje podgrupo $\langle x\rangle \cong \mathbb{Z}$. Torej se ob prehodu na podgrupo rast lahko bistveno upočasni – od eksponentne do polinomske.

Pri podgrupah končnega indeksa in kvocientih po končnih podgrupah edinkah imamo več nadzora.

Trditev. Naj bo G končno generirana grupa, $H \leq G$, $|G : H| < \infty$, $N \trianglelefteq G$, $|N| < \infty$. Tedaj so rastne funkcije grup G, H in G/N ekvivalentne. V primeru polinomske rasti je zato $\deg(G) = \deg(H) = \deg(G/N)$. Velja še implikacija $\Omega(H) > 1 \Rightarrow \Omega(G) > 1$.

Dokaz. Rastne funkcije obravnavajmo le do ekvivalence natančno. Pišimo jih zato kar kot $\beta_G, \beta_H, \beta_{G/N}$. Vemo že $\beta_H, \beta_{G/N} \leq \beta_G$. Dokaz trditve sloni na naslednjih dveh pomožnih trditvah.

Naj bo $G = \langle S\rangle$. Tedaj lahko izberemo $R \subseteq G$, ki vsebuje natanko enega predstavnika iz vsakega odseka H v G. Pri tem lahko dodatno dosežemo, da je $1 \in R$ in da velja $\max\{\ell_S(r) \mid r \in R\} < |G : H|$.

Dokaz je elementaren. (→ vaje)

Obstaja končna množica $U \subseteq H$ z lastnostjo $H = \langle U\rangle$ in $\forall h \in H\colon\ \ell_U(h) \leq \ell_S(h)$.

Dokaz: Naj bo $h \in H$. Pišimo $h = s_1 s_2 \cdots s_k$ za neke $s_i \in S \cup S^{-1}$, kjer je $k = \ell_S(h)$. Tedaj lahko po vrsti izberemo $1 = u_0, u_1, \ldots, u_{k-1}, u_k \in R$, da velja $s_i u_i^{-1} \in u_{i-1}^{-1} H$, se pravi $u_{i-1} s_i u_i^{-1} \in H$ za vsak i. Torej je

$$h u_k^{-1} = u_0 s_1 u_1^{-1} \cdot u_1 s_2 u_2^{-1} \cdots u_{k-1} s_k u_k^{-1} \in H,$$

zato je $u_k \in H$ in torej $u_k = 1$. Tako smo zapisali h kot produkt dolžine k elementov iz končne množice $U = \{xsy \mid x, y \in R \cup R^{-1},\ s \in S \cup S^{-1}\}$. Ker je bil h poljuben, od tod sledi, da množica U generira H in da pri tem velja $\ell_U(h) \leq k = \ell_S(h)$ z vsak $h \in H$. ✓✓

$\beta_G \leq \beta_H$: Označimo $C = \max\{\ell_S(r) \mid r \in R\}$. Naj bo $g \in B_{G,S}(n)$. Pišemo lahko $g = rh$ za neka $r \in R$, $h \in H$. Sledi $\ell_S(h) \leq \ell_S(g) + \ell_S(r) \leq n + C$. Zato velja tudi $\ell_U(h) \leq \ell_S(h) \leq n + C$, torej je $h \in B_{H,U}(n + C)$. Tako smo izpeljali neenakost $\beta_{G,S}(n) \leq |R| \cdot \beta_{H,U}(n + C) \leq |G : H| \cdot \beta_{H,U}((C+1)n)$. Tako je res $\beta_G \leq \beta_H$. ✓✓

$\beta_G \leq \beta_{G/N}$: Naj bo $G/N = \langle X \rangle$. Za vsak $x \in X$ izberimo dvig $\tilde{x} \in G$, torej $x = \tilde{x}N$. Naj bo $Y = \{\tilde{x} \mid x \in X\} \cup N$. Velja $G = \langle Y \rangle$. Za vsak $g \in B_{G,Y}(n)$ velja $gN \in B_{G/N,Y}(n)$, torej lahko pišemo $gN = x_1 \cdots x_k$ za nek $k \leq n$. To pomeni $g = \tilde{x}_1 \cdots \tilde{x}_k n$ za nek $n \in N$. Tako je $\beta_{G,Y}(n) \leq \beta_{G/N,X}(n) \cdot |N|$, zato je res $\beta_G \leq \beta_{G/N}$. ✓✓

$\Omega(H) > 1 \Rightarrow \Omega(G) > 1$: Naj bo $S \subseteq G$ neka generirajoča množica grupe G. Po drugi pomožni trditvi obstaja $U \subseteq H$, tako da je $\langle U \rangle = H$ in za vsak $h \in H$ velja $\ell_U(h) \leq \ell_S(h)$. Po konstrukciji množice U za vsak $u \in U$ velja $\ell_S(u) \leq 2 \cdot \max\{\ell_S(r) \mid r \in R\} + 1$, zato po prvi pomožni trditvi velja $\ell_S(u) < 2|G : H| + 1$. Tako velja $\beta_{H,U}(n) \leq \beta_{G,S}(n \cdot (2|G : H| + 1))$. Hkrati je $\beta_{H,U}(n) \geq Ac^n$, kjer je $c = \Omega(H) > 1$ odvisna le od H, konstanta A pa je morda odvisna od U. Od tod izpeljemo, da za vsak $n \in \mathbb{N}$ velja

$$\beta_{G,S}(n \cdot (2|G : H| + 1)) \geq Ac^n,$$

zato za neskončno mnogo naravnih števil m velja

$$\beta_{G,S}(m) \geq Ac^{\frac{m}{2|G:H|+1}}.$$

S tem je $\omega_S(G) \geq c^{\frac{1}{2|G:H|+1}}$, kar implicira $\Omega(G) \geq \Omega(H)^{\frac{1}{2|G:H|+1}} > 1$. ✓✓ □

Odprt problem. Ali v zadnji trditvi velja obrat zadnje implikacije? Se pravi, ali ima podgrupa končnega indeksa v grupi enakomerno eksponentne rasti tudi sama enakomerno eksponentno rast?

Zgled. Opazujmo diedrsko grupo $D_\infty = \langle s, t \mid t^2, tst^{-1} = s^{-1} \rangle$. Ta vsebuje podgrupo edinko $\langle s \rangle \cong \mathbb{Z}$ indeksa 2. Torej je D_∞ virtualno $\mathbb{Z}$. Zato sta rastni funkciji grup D_∞ in $\mathbb{Z}$ ekvivalentni. Grupa D_∞ ima tako polinomsko rast stopnje 1.

Nazadnje premislimo še, kaj se zgodi s podgrupami neskončnega indeksa v grupah polinomske rasti. Ta kriterij bo uporaben pri induktivnih sklepih v nadaljevanju.

Trditev. Bodi G grupa polinomske rasti. Naj bo H končno generirana podgrupa neskončnega indeksa v G. Tedaj je $\deg(H) \leq \deg(G) - 1$. Sorodno za vsako končno generirano neskončno podgrupo edinko N v G velja $\deg(G/N) \leq \deg(G) - 1$.

Dokaz. Dokažimo le prvi del trditve glede pogrup, drugi del glede kvocientov je mnogo lažji.

Naj bo $H = \langle T \rangle$, $G = \langle S \rangle$, privzamemo lahko $T \subseteq S$. Označimo $S = \{s_1, s_2, \ldots, s_m\}$. Opazujmo odseke H v G. Začnemo z odsekom $s_1 H$; označimo $x_1 = s_1$, opazujemo torej odsek $x_1 H$. Ker je $|G : H| = \infty$, mora vsaj en generator s_i premakniti $s_1 H$ v nek drugo odsek $s_i s_1 H$; označimo $x_2 = s_i s_1$, dobimo torej odsek $x_2 H$. Postopek generiranja novih odsekov nadaljujemo na ta način, tako dobimo paroma različne odseke $x_i H$ za $i \in \mathbb{N}$. Pri tem po konstrukciji velja $\ell_S(x_i) \leq i$. Tako za vsak $n \in \mathbb{N}$ dobimo *injektivno* preslikavo

$$\{x_1, x_2, \ldots, x_n\} \times B_{H,T}(n) \to B_{G,S}(2n), \quad (x_i, h) \mapsto x_i \cdot h.$$

Od tod sledi $n \cdot \beta_{H,T}(n) \leq \beta_{G,S}(2n)$, kar implicira $1 + \deg(H) \leq \deg(G)$. □

Zgled. Opazujmo naraščajočo verigo grup $\mathbb{Z} \leq \mathbb{Z}^2 \leq \mathbb{Z}^3 \leq \cdots$. Grupa $\mathbb{Z}^i$ v tej verigi ima polinomsko rast stopnje i.

Poglavje 5

Polinomska rast

5.1 Rast nilpotentnih grup

Polinomska rast nilpotentnih grup

V tem razdelku bomo dokazali, da so nilpotente grupe polinomske rasti. Ker sta rastni funkciji grupe in njene podgrupe končnega indeksa ekvivalentni, bomo s tem dokazali celo naslednje.

Izrek. Končno generirane virtualno nilpotentne grupe so polinomske rasti.

Dokaz. Naj bo G končno generirana nilpotentna grupa. V posebnem je G policiklična. Z indukcijo na Hirschovo dolžino $h(G)$ bomo dokazali, da je G polinomske rasti.

Baza indukcije je $h(G) = 0$. V tem primeru je grupa G končna, torej je polinomske rasti. ✓✓

Naj ima zdaj G verigo podgrup $G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_r \trianglerighteq G_{r+1} = 1$ s cikličnimi kvocienti, torej za vsak i lahko pišemo $G_i = \langle G_{i+1}, x_i \rangle$ za nek $x_i \in G$. Naj bo $X = \{x_1, \ldots, x_r\}$. Velja $G = \langle X \rangle$.

Če je $|G : G_2| < \infty$, potem lahko preidemo na grupo G_2, pri čemer sta funkciji rasti grup G in G_2 ekvivalentni. Brez škode lahko torej privzamemo, da je $G/G_2 \cong \mathbb{Z}$. S tem je $h(G_2) = h(G) - 1$, zato ima po indukciji grupa G_2 polinomsko rast.

Ocenimo vrednost $\beta_{G,X}(n)$ za poljuben $n \in \mathbb{N}$. V ta namen izberimo $x \in B_{G,X}(n)$, ki ga lahko zapišemo v obliki $x = y_1 y_2 \ldots y_n$, kjer je $y_i \in X \cup X^{-1}$. Ta element bomo prepisali v obliko $x = x_1^e \cdot z$ za neka $e \in \mathbb{Z}, z \in G_2$, in sicer z uporabo naslednjega postopka.

- *Korak 1:* V besedi $y_1 y_2 \ldots y_n$ poiščemo pojavitev simbola x_1 ali x_1^{-1}, ki je desno od nekega drugega simbola iz množice $X \cup X^{-1}$, recimo mu s.[1] Tak par zamenjamo z izrazom $x_1^{\pm 1} s [s, x_1^{\pm 1}]$. Na ta način smo element $x_1^{\pm 1}$ prestavili z desne na levo od s. Zdaj element $x_1^{\pm 1}$ še naprej potiskamo na levo, dokler levo od njega ni nobenih drugih generatorjev iz množice $X \cup X^{-1}$.

- *Korak 2:* V novi besedi poiščemo še kakšno drugo morebitno pojavitev simbola x_1 ali x_1^{-1}, ki še ni zbrana na začetku besede. Naj bo s simbol, ki je zapisan levo od $x_1^{\pm 1}$. Pri tem je $s \in X \cup X^{-1} \cup [X^{\pm 1}, X^{\pm 1}]$.

[1] Lahko se na primer zgodi, da imamo nekje v besedi pojavitev oblike $x_2 \cdot x_1$.

Tako pojavitev zopet zamenjamo z $x_1^{\pm 1} s [s, x_1^{\pm 1}]$.[2] Zdaj element $x_1^{\pm 1}$ še naprej potiskamo na levo, dokler pred njim ni niti drugih generatorjev niti komutatorjev.

• *Korak i:* V novi besedi poiščemo še kakšno drugo morebitno pojavitev simbola x_1 ali x_1^{-1}, ki še ni zbrana na začetku besede. To pojavitev potiskamo na levo z enakim postopkom, kot je opisan v prejšnjih korakih, in sicer zamenjamo vrstni red komutatorja uteži največ i z $x_1^{\pm 1}$, pri čemer uvedemo nov komutator uteži največ $i+1$ z vnosi iz množice $X \cup X^{-1}$.

Te korake izvajamo tako dolgo, dokler niso vse pojavitve x_1 in x_1^{-1} zbrane na levi strani besede. Na ta način dobimo želen zapis $x = x_1^e \cdot z$ za neka $e \in \mathbb{Z}, z \in G_2$. Pri tem lahko e in $\ell_X(z)$ omejimo na naslednji način.

- Ker je $x \in B_{G,X}(n)$, sledi $|e| \leq n$, zato imamo največ $2n+1$ možnosti za e.
- Po *Koraku 1* imamo največ n komutatorjev uteži 2.
- Po *Koraku 2* imamo največ n komutatorjev uteži 3 in največ $n+n = 2n$ komutatorjev uteži 2.[3]
- Po *Koraku 3* imamo največ n komutatorjev uteži 4, največ $n+2n = 3n$ komutatorjev uteži 3 in največ $2n+n = 3n$ komutatorjev uteži 2.
- Po *Koraku i* imamo največ $\binom{i}{k-1} \cdot n$ komutatorjev uteži k.

Število izvedenih korakov je največ n. Hkrati je grupa G nilpotentna, recimo razreda nilpotentnosti c, zato so vsi komutatorji uteži vsaj $c+1$ trivialni v G. Tako je po zadnjem koraku (*Koraku n*) element $x = x_1^e z$ zapisan kot produkt x_1^e in produkt največ $\binom{n}{k-1} \cdot n$ komutatorjev uteži k za vse $k = 1, \ldots, c$. Velja $\binom{n}{k-1} \cdot n \leq n^k$, zato je z zapisan kot produkt največ $n + n^2 + \cdots + n^c$ komutatorjev uteži kvečjemu c z vnosi iz $X \cup X^{-1}$. Vsak od teh komutatorjev uteži vsaj 2 je element podgrupe $G_2 = \langle x_2, \ldots, x_r \rangle$, saj je G/G_2 abelova grupa. Naj bo

$$A = \max\{\ell_{\{x_2,\ldots,x_r\}}(k) \mid k \in G_2 \text{ je komutator uteži} \leq c \text{ z vnosi iz } X \cup X^{-1}\}.$$

Tako za vsak dovolj velik n velja

$$\ell_{\{x_2,\ldots,x_r\}}(z) \leq n + A(n^2 + \cdots + n^c) < An^{c+1}.$$

Nazadnje torej velja

$$\beta_{G,X}(n) \leq (2n+1) \cdot \beta_{G_2,\{x_2,\ldots,x_r\}}(An^{c+1}).$$

Ker je $\beta_{G_2,\{x_2,\ldots,x_r\}}$ po indukcijski predpostavki polinom, je torej funkcija $\beta_{G,X}$ omejena s polinomom, zato je G polinomske rasti. □

[2] Lahko se na primer zgodi, da imamo nekje v besedi pojavitev oblike $x_3 \cdot x_1$ ali pa $[x_2, x_1] \cdot x_1$. Tako pojavitev zamenjamo z $x_1 x_3 [x_3, x_1]$ oziroma z $x_1 [x_2, x_1][x_2, x_1, x_1]$.

[3] Imamo namreč največ n komutatorjev uteži 2 iz prejšnjega koraka in hkrati uvedemo največ n novih komutatorjev uteži 2.

Rast Heisenbergove grupe

Zgled. Naj bo H Heisenbergova grupa. Označimo

$$x=\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix},\quad y=\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix},\quad z=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}.$$

Velja $[y,x]=z$. Dolžino elementov grupe H merimo glede na generirajočo množico $\{x,y,z\}$. Vsak element $h\in H$ lahko enolično zapišemo v obliki

$$h=\begin{pmatrix}1&b&c\\0&1&a\\0&0&1\end{pmatrix}=x^a y^b z^c.$$

Pri zbiranju kot v dokazu zadnjega izreka uporabimo naslednje lastnosti, ki veljajo v grupi H:

$$\begin{aligned}(x^a y^b z^c)\cdot x^{\pm1}&=x^{a\pm1}y^b z^{c\pm b},\\(x^a y^b z^c)\cdot y^{\pm1}&=x^{1}y^{b\pm1}z^{c},\\(x^a y^b z^c)\cdot z^{\pm1}&=x^{a}y^{b}z^{c\pm1}.\end{aligned}$$

Kaj lahko povemo o dolžini $\ell(x^a y^b z^c)$?[4]

- Prva lastnost dolžine je:

$$\boxed{\ell(x^a y^b z^c)\le|a|+|b|+6\sqrt{|c|}}$$

  Dokaz: Iz komutatorskih identitet sledi, da je komutator bilinearen v grupah razreda nilpotentnosti 2. Zato za vsak i,j velja $[y^i,x^j]=[y,x]^{ij}=z^{ij}$. Opazujmo element z^c, ki ga s pomočjo zadnjega trika prepišimo na naslednji način. Naj bo $i=\lfloor\sqrt{|c|}\rfloor$ in $j=c-i^2$. Tedaj je $z^c=z^{i^2}z^j=[y^i,x^i]z^j$, torej je $\ell(z^c)\le 4i+j\le 4\sqrt{|c|}+c-(\sqrt{|c|}-1)^2\le 6\sqrt{|c|}$. S tem je $\ell(x^a y^b z^c)\le|a|+|b|+6\sqrt{|c|}$. ✓✓

  Od tod sledi

$$\beta_H(n)\ge|\{(a,b,c)\in\mathbb{Z}^3\mid|a|+|b|+6\sqrt{|c|}\le n\}|\ge\left(\frac{n}{8}\right)\cdot\left(\frac{n}{8}\right)\cdot\left(\frac{n}{8}\right)^2,$$

  zato je $n^4\le\beta_H$.

- Druga lastnost dolžine je:

$$\boxed{\ell(x^a y^b z^c)\le n\Rightarrow|a|+|b|\le n\text{ in }|c|\le n^2}$$

  Dokaz: Predpostavimo $\ell(x^a y^b z^c)\le n$.

  $|a|+|b|\le n$: Najprej velja

$$\ell_{H,\{x,y,z\}}(x^a y^b z^c)\ge\ell_{H/H^{(2)},\{xH^{(2)},yH^{(2)}\}}(x^a y^b H^{(2)}).$$

  Ker je $H/H^{(2)}\cong\mathbb{Z}^2$, je zadnja dolžina enaka $|a|+|b|$. Tako je res $n\ge|a|+|b|$. ✓✓

[4] Pozor: v grupi H velja na primer $\ell(xyz)=\ell(yx)=2$, torej v splošnem *ni* res $\ell(x^a y^b z^c)=|a|+|b|+|c|$.

$|c| \leq n^2$: Dokazujemo z indukcijo na n. V primeru $n = 1$ je seveda $|c| \leq 1$. Predpostavimo zdaj, da trditev že velja za nek n. Naj bo $\ell(x^a y^b z^c) \leq n+1$, torej se $x^a y^b z^c$ lahko zapiše kot beseda w dolžine kvečjemu $n+1$. Ta beseda se konča z $x^{\pm 1}$, $y^{\pm 1}$ ali $z^{\pm 1}$. Torej lahko w skrajšamo za 1, če jo pomnožimo z desne z elementom $s \in \{x^{\mp 1}, y^{\mp 1}, z^{\mp 1}\}$. Tako je $\ell(x^a y^b z^c \cdot s) \leq n$. Po indukciji in zgornjih treh lastnostih množenja v grupi H je zato $|c \mp X| \leq n^2$, kjer je $X = 1$ v primeru $b = 0$ in $X = b$ sicer. Ker je $|b| \leq n$, od tod sledi $|c| \leq |X| + n^2 \leq n + n^2 < (n+1)^2$. Indukcijski korak je zaključen. ✓✓

Od tod sledi

$$\beta_H(n) \leq (2n+1) \cdot (2n+1) \cdot (2n^2+1),$$

zato je $\beta_H \preceq n^4$.

Ko obe lastnosti dolžine združimo, tako sklepamo, da je β_H ekvivalentna n^4. Pri tem smo zelo podrobno upoštevali strukturo grupe H, tako natančnega rezultata o rasti ne bi mogli dobiti le z neposredno uporabo postopka v zadnjem izreku.

Natančna stopnja rasti nilpotente grupe

Podobno analizo kot v primeru Heisenbergove grupe lahko izvedemo v splošnem[5] in tako dobimo ekspliciten opis stopnje rasti nilpotentne grupe.

Izrek. Naj bo G končno generirana nilpotentna grupa. Naj bo $r_i = h(\gamma_i(G)/\gamma_{i+1}(G))$. Tedaj je $\deg(G) = \sum_i i \cdot r_i$.

Zgled. Za Heisenbergovo grupo velja $H \geq \gamma_2(H) \geq \gamma_3(H) = 1$ s kvocientoma $\mathbb{Z}^2$ in $\mathbb{Z}$. Torej iz izreka sledi $\deg(H) = 1 \cdot 2 + 2 \cdot 1 = 4$, kot smo izračunali v prejšnjem zgledu.

5.2 Rast rešljivih grup

Rast svetilkarjeve grupe

Rešljive grupe *niso* nujno polinomske rasti.

Zgled. Naj bo L svetilkarjeva grupa. To je rešljiva grupa, ki jo predstavimo kot $L = (\bigoplus_{i \in \mathbb{Z}} \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}$. Dokažimo, da je L eksponentne rasti. V ta namen si za vsak $n \in \mathbb{N}$ oglejmo množico

$$E_n = \{(\vec{v}, m) \mid m \in \mathbb{Z},\ m \in [-n, n],\ \vec{v} \in \prod_{i \in \mathbb{Z}} \mathbb{Z}/2\mathbb{Z},\ j \notin [-n, n] \Rightarrow \vec{v}_j = 0\} \subseteq L.$$

Velja $|E_n| = 2^{2n+1}(2n+1)$. Vsak element $(\vec{v}, m) \in E_n$ si lahko predstavljamo kot svetilkarjev sprehod: svetilkar se najprej sprehodi do $-n$, potem izvede več korakov prižiganja svetilke in premikanja za 1 v levo, nazadnje pa se odpravi do svoje končne lokacije. Dolžina takega elementa je torej kvečjemu $n + 2(2n+1) + 2n = 7n + 2$. Tako za standardno množico generatorjev grupe L velja

$$\beta_L(7n+2) \geq 2^{2n+1}(2n+1).$$

Grupa L je zato res eksponentne rasti.

[5] A mi tega ne bomo naredili, primer Heisenbergove grupe bo dovolj.

Rešljive grupe podeksponentne rasti

V zadnjem primeru grupa L *ni* policiklična, take rešljive grupe pa nikdar niso niti podeksponentne rasti.

Izrek. Končno generirane rešljive grupe podeksponentne rasti so policiklične.

Izrek bomo izpeljali kot posledico naslednje trditve.

Trditev. (PODEKSPONENTNA ⇒ IZVEDENA K.G.) Bodi G končno generirana grupa podeksponentne rasti. Tedaj je grupa $[G,G]$ končno generirana.

Trditev implicira izrek. Naj bo G končno generirana rešljiva grupa podeksponentne rasti. Po trditvi je $G^{(2)}$ tudi končno generirana rešljiva grupa podeksponentne rasti, prav take so induktivno zato tudi vse podgrupe $G^{(i)}$ grupe G. Torej so kvocienti izvedene vrste $G^{(i)}/G^{(i+1)}$ končno generirane abelove grupe, zato so policiklični. Tako je tudi G policiklična grupa. □

Dokaz trditve (PODEKSPONENTNA ⇒ IZVEDENA K.G.)**.** Ker je grupa $G/[G,G]$ končno generirana abelova grupa, je policiklična. Zato bo dovolj dokazati, da za vsako podgrupo edinko $N \trianglelefteq G$ s cikličnim kvocientom G/N velja, da je N končno generirana.

Če je $|G:N| < \infty$, potem je jasno N končno generirana. Privzemimo zdaj, da je $G/N = \langle xN \rangle \cong \mathbb{Z}$ za nek $x \in G$. Naj bo $G = \langle x_1, \ldots, x_d \rangle$. Vsakega od generatorjev lahko zapišemo kot $x_i = x^{e_i} y_i$ za neka $e_i \in \mathbb{Z}$, $y_i \in N$. Jasno je $\langle\langle y_1, \ldots, y_d \rangle\rangle \leq N$. Hkrati je kvocientna grupa $G/\langle\langle y_1, \ldots, y_d \rangle\rangle$ generirana z odsekom elementa x. Torej je $G/\langle\langle y_1, \ldots, y_d \rangle\rangle$ neskončna ciklična grupa s kvocientom $G/N \cong \mathbb{Z}$. To je mogoče le v primeru $N = \langle\langle y_1, \ldots, y_d \rangle\rangle$.

Za vsak $i = 1, 2, \ldots, d$ definirajmo $K_i = \langle \{ x^n y_i x^{-n} \mid n \in \mathbb{Z} \} \rangle \leq N$. Grupa $\langle K_1, \ldots, K_d \rangle$ je edinka v G, ki je vsebovana v N, hkrati pa vsebuje vse $y_1, \ldots, y_d$. Zato je $\langle K_1, \ldots, K_d \rangle = N$.

Za vsak i je grupa K_i končno generirana: Opazujmo elemente

$$x y_i^{\alpha_1} x y_i^{\alpha_2} \cdots x y_i^{\alpha_n} \in G,$$

kjer je $\alpha_j \in \{0, 1\}$. Vseh takih besed je 2^n, vsaka od njih je dolžine kvečjemu $2n$. Iz predpostavke o podeksponentni rasti sta zato za dovolj velik n dve taki besedi enaki v G. Naj bo n_0 najmanjše naravno število, pri katerem se to zgodi. Velja torej

$$\prod_{j=1}^{n_0} x y_i^{\alpha_j} = \prod_{j=1}^{n_0} x y_i^{\beta_j}$$

za neke $\alpha_j, \beta_j \in \{0, 1\}$. Uvedimo oznako $y_i^{[k]} = x^k y_i x^{-k}$. Velja torej

$$\prod_{j=1}^{n_0} \left(y_i^{[j]} \right)^{\alpha_j} = \prod_{j=1}^{n_0} \left(y_i^{[j]} \right)^{\beta_j}.$$

Zaradi minimalnosti n_0 je pri tem $\alpha_{n_0} \neq \beta_{n_0}$, od koder sledi

$$y_i^{[n_0]} \in \langle y_i^{[1]}, y_i^{[2]}, \ldots, y_i^{[n_0-1]} \rangle.$$

Zdaj lahko izpeljemo

$$y_i^{[n_0+1]} \in x\langle y_i^{[1]}, y_i^{[2]}, \ldots, y_i^{[n_0-1]}\rangle x^{-1} = \langle y_i^{[2]}, y_i^{[3]}, \ldots, y_i^{[n_0]}\rangle \\ \leq \langle y_i^{[1]}, y_i^{[2]}, \ldots, y_i^{[n_0-1]}\rangle.$$

Induktivno sledi, da za vsak $n \geq n_0$ velja $y_i^{[n]} \in \langle y_i^{[1]}, y_i^{[2]}, \ldots, y_i^{[n_0-1]}\rangle$. Analogno lastnost lahko izpeljemo za vse dovolj majhne negativne vrednosti n.[6] Torej obstaja N_0, da za vsak $n \in \mathbb{Z}$ velja

$$y_i^{[n]} \in \langle y_i^{[-N_0]}, y_i^{[-N_0+1]}, \ldots, y_i^{[N_0]}\rangle.$$

S tem je $K_i = \langle \{y_i^{[n]} \mid n \in \mathbb{Z}\}\rangle = \langle y_i^{[-N_0]}, y_i^{[-N_0+1]}, \ldots, y_i^{[N_0]}\rangle$, torej je K_i res končno generirana grupa. □

Rast Osinove grupe

Niso vse policiklične grupe podeksponentne rasti.

Zgled. (Osin 2003)

Naj grupa $\mathbb{Z}$ deluje na $\mathbb{Z}^2$ s predpisom

$$\varphi: \mathbb{Z} = \langle s\rangle \to \mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}_2(\mathbb{Z}), \quad s \mapsto A := \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Tvorimo semidirektni produkt $\mathcal{O} = \mathbb{Z}^2 \rtimes_\varphi \mathbb{Z}$. Naj bo $S = \{e_1, e_2, s\} \subseteq \mathcal{O}$, kjer sta e_1, e_2 standardna bazna vektorja v $\mathbb{Z}^2$.

Oglejmo si elemente grupe $\mathcal{O}$ oblike

$$g_{\epsilon_0,\ldots,\epsilon_n} = \sum_{j=0}^{n} A^j(\epsilon_j e_1) \in \mathbb{Z}^2 \leq \mathcal{O}$$

za $n \geq 1$ in $\epsilon_i \in \{0,1\}$.

Za fiksno vrednost n so vsi ti elementi različni med sabo: Naj bo $\Lambda = \frac{3+\sqrt{5}}{2}$ največja lastna vrednost matrike A s pripadajočim lastnim vektorjem $w = (\frac{1+\sqrt{5}}{2}, 1) \in \mathbb{R}^2$. Definirajmo linearno preslikavo

$$L: \mathbb{C}^2 \to \mathbb{C}, \quad v \mapsto \langle w, v\rangle.$$

Za vsak $v \in \mathbb{C}^2$ velja račun $LAv = \langle w, Av\rangle = \langle A^T w, v\rangle = \langle \Lambda w, v\rangle = \Lambda \cdot Lv$. Če torej na enem od opazovanih elementov uporabimo L, sledi

$$L(g_{\epsilon_0,\ldots,\epsilon_n}) = \sum_{j=0}^{n} \Lambda^j \cdot L(\epsilon_j e_1) = \frac{1+\sqrt{5}}{2} \cdot \sum_{j=0}^{n} \Lambda^j \epsilon_j.$$

Ker je $\Lambda > 2$, lahko iz števila $\sum_{j=0}^{n} \Lambda^j \epsilon_j$ enolično izračunamo vrednosti $\epsilon_0, \ldots, \epsilon_n$.[7] ✓

Torej je število vseh opazovanih elementov enako

$$|\{g_{\epsilon_0,\ldots,\epsilon_n} \mid \epsilon_i \in \{0,1\}\}| = 2^{n+1}.$$

Hkrati lahko vsak tak element zapišemo v multiplikativni obliki

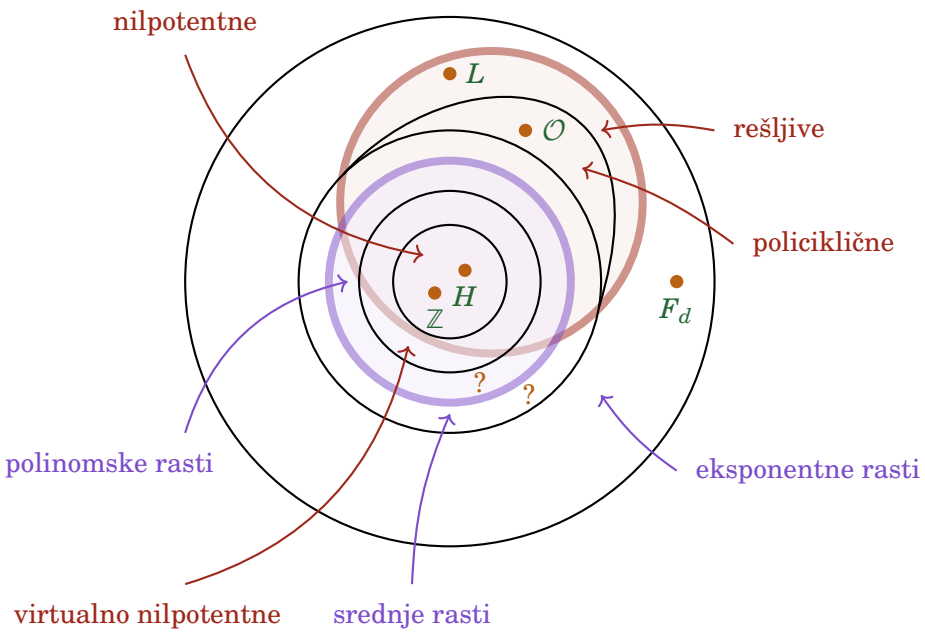
$$g_{\epsilon_0,\ldots,\epsilon_n} = \prod_{j=0}^{n} s^j e_1^{\epsilon_j} s^{-j} = e_1^{\epsilon_0} s e_1^{\epsilon_1} s \cdots s e_1^{\epsilon_n} s^{-n},$$

kjer smo upoštevali, da v grupi $\mathcal{O}$ velja račun $s e_1 s^{-1} = \varphi(s).e_1 = A e_1$.

Velja torej $\ell_S(g_{\epsilon_0,\ldots,\epsilon_n}) \leq 1 + 2n + n = 3n + 1$. S tem je $\beta_{\mathcal{O},S}(3n+1) \geq 2^{n+1}$ in grupa $\mathcal{O}$ je zato eksponentne rasti.

[6] To storimo tako, da v dokazu x zamenjamo z x^{-1}.

[7] Vrednosti izračunamo induktivno, najprej izračunamo ϵ_n, po tem $\epsilon_{n-1}, \ldots$ Ta postopek je kot pri izračunu števk števila v dvojiškem zapisu.



Slika 5.1: Diagram grup različnih rasti in njihove algebraične strukture

Oddih in razgled

Do zdaj smo dokazali, da so virtualno nilpotentne grupe (na primer H) polinomske rasti in da so rešljive grupe podeksponentne rasti nujno policiklične. Podali smo primer rešljive grupe eksponentne rasti (L) in policiklične grupe eksponentne rasti ($\mathcal{O}$).

Pri tem se porodita naslednji naravni vprašanji.

1. (POLI. IN NE V. NILP.) Primer grupe polinomske rasti, ki ni virtualno nilpotentna?

2. (SREDNJA) Primer grupe srednje rasti?

Policiklične grupe podeksponentne rasti

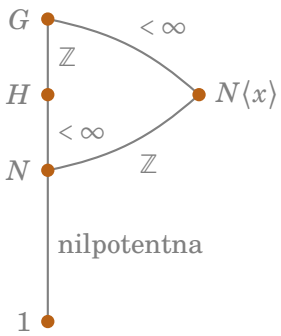
Dokazali bomo[8], da v rešljivih grupah ne moremo najti primerov, ki bi odgovorili na zastavljeni vprašanji.

Izrek. Policiklična grupa podeksponentne rasti je virtualno nilpotentna, torej v posebnem polinomske rasti.

Dokaz. Naj bo G policiklična grupa podeksponentne rasti. Po potrebi G zamenjamo s podgrupo končnega indeksa, tako da bo G imela edinko $H \trianglelefteq G$ z $G/H = \langle xH \rangle \cong \mathbb{Z}$ za nek $x \in G$ in torej $h(H) < h(G)$. Po indukciji na Hirschovo dolžino lahko predpostavimo, da je H virtualno nilpotentna. Torej obstaja nilpotentna podgrupa $N \leq H$ končnega indeksa v H. Po potrebi N zamenjamo s presekom vseh podgrup indeksa $|H : N|$ v H in zato lahko predpostavimo, da vsak avtomorfizem H ohranja N, torej v posebnem velja $N \trianglelefteq G$.

[8] Dokaz je nekoliko zahteven.

Opazujmo podgrupo $N\langle x\rangle \leq G$. Velja $G/N = H/N \cdot \langle x\rangle N/N$, zato je $|G : N\langle x\rangle| \leq |H : N| < \infty$. Hkrati je $N\langle x\rangle/N \cong \langle x\rangle/(\langle x\rangle \cap N) = \langle x\rangle \cong \mathbb{Z}$. Brez škode lahko zato grupo G nadomestimo z grupo $N\langle x\rangle$ in torej predpostavimo, da je G razširitev grupe $\langle x\rangle \cong \mathbb{Z}$ z nilpotentno grupo N. Radi bi našli nilpotentno podgrupo končnega indeksa v G. V ta namen dokažimo naslednjo pomožno trditev.



> Naj bo G razširitev grupe $\langle x\rangle \cong \mathbb{Z}$ z nilpotentno grupo N. Tedaj obstajata centralna vrsta $N = N_1 \geq N_2 \geq \cdots \geq N_\ell = 1$ edink v G in število $k \in \mathbb{Z}$, tako da je inducirano delovanje elementa x^k na vsakem kvocientu N_i/N_{i+1} trivialno.

V trditvi element x^k deluje s konjugiranjem na N_i, torej deluje tudi na kvocientu N_i/N_{i+1}. Trivialnost tega delovanja pomeni, da za vsak $n \in N_i$ velja $x^k n x^{-k} N_{i+1} = nN_{i+1}$, kar je enakovredno $[x^k, N_i] \subseteq N_{i+1}$.

Pomožna trditev implicira izrek: Res, naj bo $K = N\langle x^k\rangle$. Tedaj je vrsta $K \trianglerighteq N_1 \trianglerighteq N_2 \trianglerighteq \cdots \trianglerighteq N_\ell = 1$ centralna, saj iz komutatorskih identitet sledi $[K, N_i] \subseteq [N, N_i][x^k, N_i] \subseteq N_{i+1} \cdot N_{i+1} \subseteq N_{i+1}$. Tako je grupa K nilpotentna. Hkrati je $|G : K| = |\langle x\rangle : \langle x^k\rangle| = k$. ✓

Dokaz pomožne trditve: Grupa N je nilpotentna, zato ima centralno vrsto $N = N_1 \geq N_2 \geq \cdots \geq 1$, za katero velja celo $N_i \trianglelefteq G$,[9] vzamemo lahko na primer kar $N_i = \gamma_i(N)$. Med vsemi vrstami izberimo tako, ki ima maksimalno število neskončnih kvocientov.[10] Dobljeno vrsto lahko po potrebi še pofinimo in predpostavimo, da so vsi kvocienti bodisi končni bodisi proste abelove grupe. Dobljeno vrsto označimo z $N = N_1 \geq N_2 \geq \cdots \geq N_\ell = 1$. Dokazali bomo, da ima slednja vrsta želeno lastnost iz pomožne trditve. Pred tem zabeležimo še eno lastnost te vrste. Po maksimalnosti izbire vrste je za vsako edinko $M \trianglelefteq G$, za katero je $N_{i+1} \leq M \leq N_i$, vsaj ena od grup M/N_{i+1}, N_i/M končna.

Za dokaz pomožne trditve bo za vsak $1 \leq i \leq \ell$ dovolj najti $k_i \in \mathbb{Z}$, tako da element x^{k_i} deluje trivialno na N_i/N_{i+1}. Potem lahko namreč vzamemo $k = \prod_{i=1}^{\ell} k_i$. Pribijmo zato nek i in opazujmo N_i/N_{i+1}. Če je slednja grupa končna, potem lahko vzamemo $k_i = |\mathrm{Aut}(N_i/N_{i+1})| < \infty$. Predpostavimo zdaj, da je N_i/N_{i+1} prosta abelova grupa ranga r za nek $r \in \mathbb{N}$. To grupo obravnavajmo kot modul M nad polinomskim kolobarjem $\mathbb{Z}[X]$, kjer naj X deluje kot x. Razširimo M do vektorskega prostora $V = \mathbb{Q} \otimes_{\mathbb{Z}} M$.

> V je enostaven $\mathbb{Q}[X]$-modul.

Dokaz: Naj bo $0 \neq W \leq V$ podmodul. Za $0 \neq w \in W$ obstaja $n \in \mathbb{N}$, da je $0 \neq nw \in M$.[11] Torej je $M \cap W \neq 0$. Zato je $M \cap W$ neskončna abelova grupa. Po zgornjem komentarju o maksimalnosti izbire vrste velja, da je $M/(M \cap W)$ končna grupa. Tako je tudi $V/(M \cap W)$ torzijska grupa. S tem

[9] Torej vsak člen verige ni le edinka v N, ampak celo v G.

[10] To število je gotovo kvečjemu $h(N)$.

[11] Vsak vektor $v \in V$ je $\mathbb{Q}$-linearna kombinacija elementov M, torej obstaja $n \in \mathbb{N}$, da je $nv \in M$. Tako je grupa V/M torzijska abelova grupa. Na primer, če je $M = \mathbb{Z}$, potem je $V = \mathbb{Q}$ in $V/M = \mathbb{Q}/\mathbb{Z}$.

je tudi V/W torzijska abelova grupa, ki pa je hkrati vektorski prostor nad $\mathbb{Q}$. To je mogoče le, če je $W = V$. ✓✓

(SCHUROVA LEMA) $\mathrm{End}_{\mathbb{Q}[X]}(V)$ je obseg.

Dokaz: Naj bo $0 \neq \alpha \in \mathrm{End}_{\mathbb{Q}[X]}(V)$. Tedaj je $\ker \alpha \neq V$ in $\mathrm{im}\,\alpha \neq 0$. Ker je V enostaven, od tod sledi $\ker \alpha = 0$ in $\mathrm{im}\,\alpha = V$. Tako je α bijekcija. ✓✓

Endomorfizme $\mathrm{End}_{\mathbb{Q}[X]}(V)$ obravnavamo kot podmnožico $\mathrm{End}_{\mathbb{Q}}(V)$, kar lahko z izbiro baze prostora V identificiramo s kolobarjem matrik $\mathrm{Mat}_r(\mathbb{Q})$. Naj bo $\alpha \in \mathrm{End}_{\mathbb{Q}[X]}(V)$, ki ustreza delovanju x na $M = N_i/N_{i+1}$. Torej lahko α vidimo kot matriko v $\mathrm{Mat}_r(\mathbb{Z})$. Ta matrika je ničla svojega karakterističnega polinoma $p \in \mathbb{Z}[\lambda]$.[12] Naj bo F podobseg obsega $\mathrm{End}_{\mathbb{Q}[X]}(V)$, generiran z elementom α. Torej je $F/\mathbb{Q}$ razširitev polj z elementom α, ki je ničla polinoma p s celimi koeficienti. Zato lahko F vložimo v $\mathbb{C}$, in sicer tako, da izberemo eno ničlo $\alpha_0 \in \mathbb{C}$ polinoma p in preslikamo $\alpha \mapsto \alpha_0$.[13]

Naj bo $\tau \in \mathbb{C}$ algebraično celo število. Predpostavimo, da za vsak $\sigma \in \mathrm{Gal}(\mathbb{Q}(\tau)/\mathbb{Q})$ velja $|\sigma(\tau)| \leq 1$. Tedaj obstaja $k \in \mathbb{N}$, da je $\tau^k = 1$.

Dokaz: Naj bo ρ poljubna potenca elementa τ. Torej imajo tudi vsi konjugati ρ absolutno vrednost kvečjemu 1. Naj bo $n = |\mathbb{Q}(\tau) : \mathbb{Q}|$. Torej je $|\mathbb{Q}(\rho) : \mathbb{Q}| \leq n$, zato je minimalni polinom elementa ρ stopnje največ n, njegovi koeficienti pa so simetrične funkcije konjugatov ρ. Tako je k-ti koeficient minimalnega polinoma po absolutni vrednosti enak kvečjemu $\binom{n}{k}$. Ker je ρ algebraično celo število, so vsi koeficienti minimalnega polinoma celi. Zato obstaja le končno mnogo možnosti za minimalni polinom, torej tudi le končno mnogo možnosti za ρ. Torej obstaja le končno mnogo različnih potenc elementa τ, zato obstaja $k \in \mathbb{N}$, da je $\tau^k = 1$. ✓✓

Premislimo, da število $\alpha_0 \in \mathbb{C}$ zadošča zgornjim pogojem. Od tod bo sledilo, da obstaja $k \in \mathbb{N}$, da je $\alpha_0^k = 1$, zato je $\alpha^k = \mathrm{id}_V$ in torej x^k deluje trivialno na N_i/N_{i+1}, kar smo želeli preveriti. V ta namen predpostavimo, da α_0 ne zadošča pogojem leme. Torej je nujno $|\alpha_0| > 1$. Po potrebi nadomestimo x in α_0 z njuno potenco, da bo veljalo celo $|\alpha_0| > 2$. Izberimo $0 \neq v \in M$, ki mu ustreza $y \in N_i/N_{i+1}$. Označimo $y^{[n]} = x^n.y$ za $n \in \mathbb{N}_0$. Iz predpostavke o podeksponentni rasti zdaj kot v dokazu trditve (PODEKSPONENTNA ⇒ IZVEDENA K.G.) sledi, da obstaja $n_0 \in \mathbb{N}$, za katerega je

$$y^{[n_0]} = \sum_{i=0}^{n_0-1} c_i y^{[i]}$$

za neke $c_i \in \mathbb{Z}$, $|c_i| \leq 1$. To enakost lahko zapišemo kot

$$\alpha^{n_0}(v) = \left(\sum_{i=0}^{n_0-1} c_i \alpha^i \right)(v).$$

S tem ima endomorfizem $\alpha^{n_0} - \sum_{i=0}^{n_0-1} c_i \alpha^i \in \mathrm{End}_{\mathbb{Q}[X]}(V)$ netrivialno jedro. (SCHUROVA LEMA) zato implicira, da je ta element trivialen. Od tod

[12] Algebraičnemu številu $\tau \in \mathbb{C}$, katerega karakteristični polinom ima celoštevilske koeficiente, rečemo algebraično celo število.

[13] Ni vsaka izbira α_0 dobra, če polinom p ni nerazcepen. V tem primeru moramo obravnavati minimalni polinom elementa α. Koeficienti slednjega so po Gaussovi lemi tudi cela števila.

izpeljemo protislovje

$$|\alpha_0^{n_0}| = \left|\sum_{i=0}^{n_0-1} c_i \alpha_0^i\right| \leq \sum_{i=0}^{n_0-1} |\alpha_0|^i = \frac{|\alpha_0|^{n_0}-1}{|\alpha_0|-1} < |\alpha_0|^{n_0},$$

kjer smo v zadnji neenakosti upoštevali $|\alpha_0| > 2$. Dokaz pomožne trditve je s tem zaključen. □

5.3 Rast linearnih grup

V tem razdelku bomo večino dokazov izpustili in le našteli nekaj težkih orodij, s pomočjo katerih bomo nazadnje podali odgovor na vprašanje (POLI. IN NE V. NILP).

Upodobitve grup

Naj bo G grupa. Upodobitev grupe G je homomorfizem

$$\rho: G \to \mathrm{GL}_n(F)$$

za neko naravno število n in polje F. Običajno vzamemo kar $F = \mathbb{C}$ in v tem primeru obravnavamo kompleksne upodobitve. Upodobitvam nad polji neničelne karakteristike rečemo modularne upodobitve.

Zgled.

- Diedrsko grupo $D_{2n} = \langle s, t\rangle$ lahko upodobimo pred njenega delovanja na ravnini – element s predstavlja rotacijo za kot $2\pi/n$, element t pa zrcaljenje:

$$\rho: D_{2n} \to \mathrm{GL}_2(\mathbb{C}), \quad s \mapsto \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}, \quad t \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- Svetilkarjevo grupo $L = \langle a, t\rangle$ smo upodobili v matrikah nad poljem racionalnih funkcij nad $\mathbb{Z}/2\mathbb{Z}$:

$$\rho: L \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}(x)), \quad a \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad t \mapsto \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}.$$

- Ciklično grupo $\mathbb{Z}/20\mathbb{Z}$ lahko upodobimo nad končnim poljem $\mathbb{Z}/5\mathbb{Z}$:

$$\rho: \mathbb{Z}/20\mathbb{Z} \to \mathrm{GL}_1(\mathbb{Z}/5\mathbb{Z}) = (\mathbb{Z}/5\mathbb{Z})^*, \quad 1 \mapsto 2.$$

  Ker je $2^{20} \equiv 1 \pmod 5$, je s tem res definiran homomorfizem.

- Obstajajo grupe, ki nimajo nobene netrivialne upodobitve. Konkreten primer take grupe je Tarskijeva pošast. Naj bo p fiksno praštevilo, večje od 10^{75}. Tarskijeva pošast je neskončna grupa, v kateri je vsaka prava netrivialna podgrupa izomorfna ciklični grupi $\mathbb{Z}/p\mathbb{Z}$. Take grupe obstajajo (Olshanskii 1979). Ni težko preveriti (→ vaje), da je Tarskijeva pošast generirana z dvema elementoma in da je enostavna. Vsaka njena upodobitev $\rho: T \to \mathrm{GL}_n(F)$ bi zato morala biti bodisi injektivna bodisi trivialna. V primeru $n = 1$ bi tako z netrivialno upodobitvijo dobili vložitev T v F^*, kar ni mogoče, ker T ni abelova. Zakaj T ni mogoče vložiti v $\mathrm{GL}_n(F)$? V naslednjem razdelku bomo predstavili posebno lastnost podgrup $\mathrm{GL}_n(F)$, ki ji T ne zadošča.

Linearne grupe

Grupi G, ki ima kakšno injektivno upodobitev, rečemo linearna grupa.

Zgled.

- $\mathrm{SL}_2(\mathbb{Z})$ se naravno vloži v $\mathrm{GL}_2(\mathbb{C})$.
- Heisenbergova grupa H se naravno vloži v $\mathrm{GL}_3(\mathbb{C})$.
- Svetilkarjeva grupa L se vloži v $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}(x))$.
- Če ima enostavna grupa kakšno netrivialno upodobitev, potem je linearna.

Linearne grupe imajo naslednjo strukturno lastnost.

Izrek. (TITSOVA ALTERNATIVA) Naj bo G končno generirana linearna grupa. Potem bodisi G vsebuje prosto podgrupo (ranga vsaj 2) bodisi je G virtualno rešljiva.

V dokazu se prostost podgrupe dokaže s pomočjo izreka (PINGPONG), a je *pingpong miza*, ki jo za to potrebujemo, zgrajena iz matrik nad normiranimi napolnitvami polj. Za dokaz bi potrebovali kar veliko ozadja iz te teorije, zato ga izpustimo.

Zgled.

- Grupa $\mathrm{SL}_2(\mathbb{Z})$ vsebuje prosto grupo F_2.
- Grupi H in L sta rešljivi.
- Naj bo T Tarskijeva pošast. Če bi bila T linearna, potem bi morala bodisi vsebovati prosto podgrupo (nemogoče, saj ima T torzijske elemente, hkrati pa je vsaka prava podgrupa T ciklična) bodisi bi T morala biti virtualno rešljiva (nemogoče, saj je T enostavna, hkrati pa je indeks vsake prave podgrupe T neskončen). Torej T *ni* linearna.

Iz že dokazane lastnosti o rastnih funkcijah rešljivih grup zdaj sledi enaka lastnost za linearne grupe.

Posledica. Rastna funkcija končno generirane linearne grupe je bodisi eksponentna bodisi polinomska. Slednji primer je mogoč le, ko je grupa virtualno nilpotentna.

Torej tudi v svetu linearnih grup ne moremo najti primerov, ki bi odgovorili na vprašanj (POLI. IN NE V. NILP) in (SREDNJA).

Končne linearne grupe

Vsaka končna grupa G deluje na sebi s Cayleyjevim delovanjem in ima zato upodobitev

$$G \to \mathrm{GL}_{|G|\times|G|}(\mathbb{C}), \quad g \mapsto (e_x \mapsto e_{gx}),$$

kjer smo z $\{e_g \mid g \in G\}$ označili bazo prostora $\mathbb{C}^{|G|}$. Dimenzija upodobitve je v tem primeru seveda odvisna od velikosti grupe.

Kadar imamo dano dimenzijo vektorskega prostora, na njem lahko delujejo je končne grupe, ki so virtualno (v odvisnosti od dimenzije) abelove.

Izrek. (Jordan 1878) Naj bo F polje karakteristike 0. Če je G končna podgrupa $\mathrm{GL}_n(F)$, potem obstaja abelova edinka $A \trianglelefteq G$, da je indeks $|G:A|$ omejen s funkcijo, odvisno le od n in ne od grupe G.

Liejeve grupe

Naj bo $G \leq \mathrm{GL}_n(\mathbb{R})$ ali $G \leq \mathrm{GL}_n(\mathbb{C})$. Če je G celo zaprta v ambientalni matrični grupi, potem G podeduje topologijo in jo lahko vidimo kot podmnogoterost v $\mathbb{R}^{n^2}$ oziroma $\mathbb{C}^{n^2}$. Množenje in invertiranje v G sta analitični operaciji glede na to topološko strukturo.

Te koncepte lahko posplošimo na naslednji način. Rečemo, da je množica G topološka grupa, če je hkrati grupa in topološki prostor, operaciji množenja in invertiranja pa sta *zvezni* preslikavi. Liejeva grupa je topološka grupa, ki je kot topološki prostor *analitična mnogoterost*,[14] operaciji množenja in invertiranja pa sta *analitični*.

Zgled.

- $\mathrm{GL}_n(\mathbb{R})$ je realna Liejeva grupa, $\mathrm{GL}_n(\mathbb{C})$ pa je kompleksna Liejeva grupa.
- $S^1 \subseteq \mathbb{R}^2$ je realna Liejeva grupa.
- Zvezna Heisenbergova grupa je grupa

$$H_{\mathbb{R}} = \left\{ \begin{pmatrix} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} \mid a,b,c \in \mathbb{R} \right\}.$$

  Ta grupa je realna Liejeva grupa.
- Grupa $(\mathbb{Q},+)$, opremljena s topologijo na $\mathbb{R}$, je topološka grupa, ki pa *ni* Liejeva grupa.

Liejeve grupe sicer niso vedno linearne,[15] so pa zelo blizu temu, kot prikaže naslednja trditev.[16]

Trditev. Bodi G Liejeva grupa s končno mnogo komponentami.

1. Obstaja abelova edinka $Z \trianglelefteq G$, tako da je G/Z kompleksna linearna grupa.
2. (brez malih redov) Za vsak $n \in \mathbb{N}$ obstaja $U \subseteq_o G$, $1 \in U$, tako da U *ne* vsebuje nobenega netrivialnega elementa reda kvečjemu n.

[14] To pomeni, da je topološki prostor pokrit z odprtimi množicami $\{U_i\}_i$, ki so homeomorfne odprtim podmnožicam v $\mathbb{R}^n$ oziroma $\mathbb{C}^n$, in to na *analitično usklajen* način: če je $U_i \cap U_j \neq \emptyset$, potem naj bo $\varphi_k : U_k \to V_k \subseteq \mathbb{R}^n$ homeomorfizem za $k \in \{i,j\}$; zahteva o analitični usklajenosti pomeni, da je prehodna preslikava $\varphi_{ij} : \varphi_i(U_i \cap U_j) \to \varphi_j(U_i \cap U_j)$, $\varphi_{ij} = \varphi_j \circ \varphi_i^{-1}$, analitična.

[15] Z nekoliko dodatnega znanja o Liejevih grupah in njihovih prirejenih Liejevih algebrah je mogoče premisliti, da je grupa $H_{\mathbb{R}}/\{I + nE_{3,3} \mid n \in \mathbb{Z}\}$ Liejeva grupa, ki *ni* linearna.

[16] V trditvi lahko za Z vzamemo povezano komponento centra G, upodobitev grupe G/Z pa izhaja iz delovanja grupe G na svoji Liejevi algebri. Druga lastnost trditve je sorodna znani lastnosti *brez malih podgrup*, angleško *no small subgroups*.

Zgled. Naj bo $G = \mathrm{GL}_n(\mathbb{R})$. Poglejmo si idejo dokaza, da ta grupa zadošča drugi lastnosti trditve. Iz ideje ni težko sestaviti natančnega argumenta (→ vaje).

Naj bo U odprta množica tistih matrik v $\mathrm{GL}_n(\mathbb{R})$, ki imajo vse lastne vrednosti *zelo blizu* 1.

Naj bo $1 \neq g \in U$. Če ima g kakšno lastno vrednost, ki je različna od 1, potem nobena majhna potenca g ni enaka 1. ✓✓ Če pa so vse lastne vrednosti g enake 1, potem je g podobna netrivialni zgornje trikotni matriki z 1 po diagonali, zato je $\lim_{m\to\infty} ||1 - g^m|| = \infty$. ✓✓

Liejeve grupe se naravno pojavijo vselej, kjer so dovolj lepi topološki prostori. To nam zagotovi naslednji globok izrek.[17]

Izrek. (Montgomery–Zippin 1955) Naj bo T *končno dimensionalen*, lokalno kompakten, povezan, lokalno povezan, *homogen* metrični prostor. Tedaj lahko grupo izometrij $\mathrm{Isom}(T)$ dodatno opremimo s strukturo Liejeve grupe s končno mnogo komponentami.

Spomnimo se na pomen homogenosti in dimenzije.

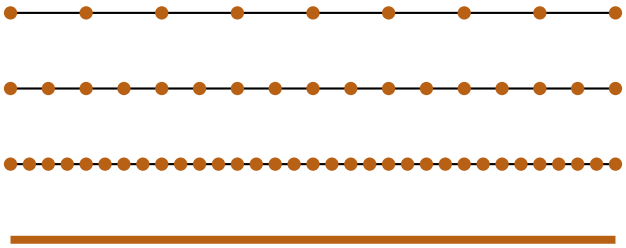
- Rečemo, da je T *homogen*, če za vsaka $x, y \in T$ obstaja $\varphi \in \mathrm{Isom}(T)$ z lastnostjo $\varphi(x) = y$.[18]
- Rečemo, da ima T *dimenzijo* 0, če za vsak $x \in T$ in vsako okolico $x \in V \subseteq_o T$ obstaja $U \subseteq_o T$, $\overline{U} \subseteq V$, da je $x \in U$, $\partial U = \varnothing$.[19]
- Induktivno rečemo, da ima T *dimenzijo kvečjemu* n, če za vsak $x \in T$ in vsako okolico $x \in V \subseteq_o T$obstaja $U \subseteq_o T$, $\overline{U} \subseteq V$, da je $x \in U$, ∂U pa ima dimenzijo kvečjemu $n-1$.[20]
- Če T nima dimenzije kvečjemu n za vsak n, potem rečemo, da ima T *neskončno dimenzijo*. V nasprotnem primeru je *dimenzija* topološkega prostora T tako število n, za katerega ima T dimenzijo kvečjemu n, nima pa dimenzije kvečjemu $n-1$. [21]

Zgled. Naj bo T običajna sfera v prostoru, $T = S^2 \subseteq \mathbb{R}^3$. Grupa izometrij $\mathrm{Isom}(T)$ sestoji iz rotacij sfere in zrcaljenj. Imenujemo jo ortogonalna grupa in označimo z $O(3)$. Velja

$$O(3) = \{Q \in \mathrm{GL}_3(\mathbb{R}) \mid Q^T Q = QQ^T = I\} \subseteq_z \mathrm{GL}_3(\mathbb{R}).$$

Grupa $O(3)$ je Liejeva grupa z dvema komponentama, ki ustrezata $\det Q = 1$ oziroma $\det Q = -1$. Komponenti z $\det Q = 1$ rečemo specialna ortogonalna grupa, oznaka $SO(3)$. Elementi grupe $SO(3)$ so rotacije prostora, torej so določeni z osjo rotacije (torej vektorjem v S^2) in s kotom rotacije (torej s številom med $-\pi$ in π). Topološko je $SO(3)$ torej krogla polmera π, kjer identificiramo antipodne točke. Torej je $SO(3)$ homeomorfna 3-dimenzionalnemu projektivnemu prostoru $\mathbb{R}P^3$.

[17] Ta izrek hkrati predstavlja razrešitev znamenitega *Hilbertovega petega problema*.
[18] Na primer, $\mathbb{R}^2$ in $\mathrm{GL}_n(\mathbb{R})$ sta homogena prostora.
[19] Na primer, $\mathbb{R}\setminus\mathbb{Q}$ s topologijo z $\mathbb{R}$ ima dimenzijo 0.
[20] Na primer, $\mathbb{R}^n$ ima dimenzijo kvečjemu n.
[21] Induktivno sledi, da je dimenzija $\mathbb{R}^n$ enaka n.



Slika 5.2: Ko graf $\mathrm{Cay}(\mathbb{Z}, \{1\})$ pogledamo od daleč, vidimo realno premico

Izrek Gromova

Z uporabo izreka (Montgomery–Zippin 1955) je Gromov dokazal naslednji izrek, ki razreši vprašanje (POLI. IN NE V. NILP.).

Izrek. (Gromov 1981) Grupe polinomske rasti so virtualno nilpotentne.

Izrek bomo dokazali v celoti (modulo nedokazane trditve iz tega razdelka). Ideja Gromova je v tem, da grupi priredi *zvezen geometrijski objekt* (imenovan asimptotski stožec), na katerem grupa deluje. Pod predpostavko polinomske rasti ima ta objekt *dobre topološke lastnosti*, zato njegova grupa izometrij tvoji *Liejevo grupo*, ki je zelo blizu tega, da bi bila *linearna*. V svetu linearnih grup pa zaradi dokazanih rezultatov o rešljivih grupah in Titsovi alternativi že vemo, da *polinomska rast implicira virtualno nilpotentnost*.

5.4 Asimptotski stožec

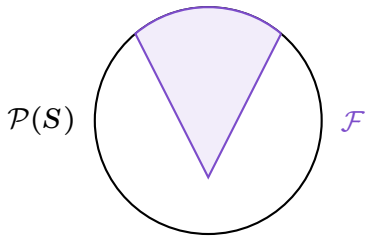
Pogled od daleč

Grupi sicer lahko priredimo Cayleyjev graf, na katerem deluje, a je ta topološki prostor, v katerem so točke vozlišča grafa, *diskreten*. Če v ta prostor dodamo še povezave grafa, potem v večini primerov ne dobimo *homogenega* metričnega prostora. Ideja Gromova je v tem, da opazujmo Cayleyjev graf grupe *od daleč*.

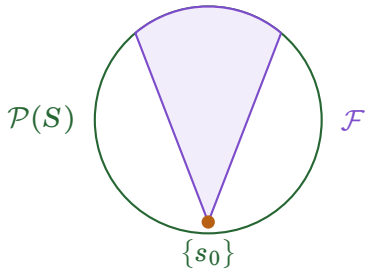
Zgled.

- Cayleyjev graf grupe $\mathbb{Z}$ sestoji iz vozlišč, indeksiranih z $\mathbb{Z}$, ki so med sabo zaporedno povezana. Ko na ta graf pogledamo od daleč, se razdalje med vozlišči skrčijo. V limiti vidimo realno premico $\mathbb{R}$.
- Cayleyjev graf grupe $\mathbb{Z}^2$ je mreža v $\mathbb{R}^2$. Ko skrčimo razdalje med vozlišči, v limiti vidimo ravnino $\mathbb{R}^2$.

Za vsako grupo lahko v Cayleyjev graf uvedemo nove metrike med vozlišči, ki skrajšajo razdalje za faktor $\frac{1}{2}, \frac{1}{3}, \ldots$ Gromov je uspel konstruirati *limitni objekt*, h kateremu ti metrični prostoru *konvergirajo*. V tem objektu so razdalje med originalnimi vozlišči grafa enake 0 in iz diskretnih prostorov dobimo *zveznega*. Originalna grupa deluje na tem objektu z izometrijami. Limitni objekt bomo imenovali asimptotski stožec. Za natančno konstrukcijo bomo potrebovali nekaj priprave.



Slika 5.3: Filter je zaprt za preseke in navzgor zaprt



Slika 5.4: Glavni ultrafilter

Ultrafiltri

Naj bo S množica. Filter na S je družina podmnožic $\mathcal{F} \subseteq \mathcal{P}(S)$, ki zadošča naslednjim pogojem:

- $\emptyset \notin \mathcal{F}$,
- $A, B \in \mathcal{F} \Rightarrow A \cap B \in \mathcal{F}$, (zaprt za preseke)
- $A \in F, A \subseteq B \Rightarrow B \in \mathcal{F}$. (navzgor zaprt)

Filtre na S lahko uredimo glede na relacijo inkluzije. Maksimalen filter se imenuje ultrafilter.

Zgled. Naj bo $s_0 \in S$. Definirajmo $\mathcal{F} = \{A \in \mathcal{P}(S) \mid s_0 \in A\}$. To je ultrafilter na S. Če je namreč $\emptyset \neq B \notin \mathcal{F}$, potem je $B \cap \{s_0\} = \emptyset$, zato noben filter, ki je večji od $\mathcal{F}$, ne vsebuje B. Ultrafiltru, konstruiranem na tak način, rečemo glavni ultrafilter.

Kadar je S končna množica, je vsak ultrafilter na njej glavni.[22] Nasprotno pa v primeru, ko je S neskončna množica, vselej obstaja neglavni ultrafilter, ki ga lahko dobimo na naslednji način. Naj bo

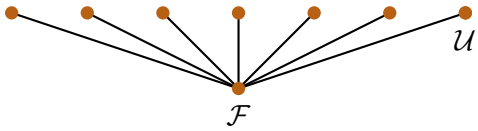
$$\mathcal{F} = \{A \in \mathcal{P}(S) \mid |S \setminus A| < \infty\},$$

to je kokončni filter. Po Zornovi lemi obstaja maksimalen filter $\mathcal{U}$, ki vsebuje $\mathcal{F}$. Filter $\mathcal{U}$ je ultrafilter, ki pa *ni* glavni.[23] Ni težko premisliti (→ vaje), da velja tudi obratno: vsak neglavni ultrafilter vsebuje kokončni ultrafilter in presek vseh neglavnih ultrafiltrov je ravno kokončni ultrafilter. Poznana ni *nobena eksplicitna konstrukcija* neglavnega ultrafiltra. Vemo le, da ti objekti obstajajo.

Ultrafiltre uporabljamo, kadar želimo razdeliti vse podmnožice množice S na bodisi *velike* (tiste v ultrafiltru) bodisi *majhne* (tisti izven ultrafiltra), pri čemer uporabljamo bolj natančen pomen majhnega kot le *končno mnogo elementov* (ta definicija majhnega ustreza kokončnemu filtru).

[22] Če je namreč $\mathcal{F}$ neglavni ultrafilter, potem za vsak $s_0 \in S$ obstaja $A_{s_0} \in \mathcal{F}$, da je $s_0 \notin A_{s_0}$. Zato je $\emptyset = \bigcap_{s_0 \in S} A_{s_0} \in \mathcal{F}$, kar je nemogoče.

[23] Za vsak $s_0 \in S$ imamo množico $S \setminus \{s_0\} \in \mathcal{F} \subseteq \mathcal{U}$, ki ne vsebuje s_0.



Slika 5.5: Presek neglavnih ultrafiltrov je kokončni filter

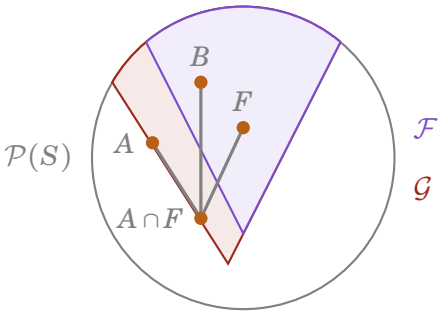
Trditev. (OSNOVNE LASTNOSTI ULTRAFILTROV)

1. Filter $\mathcal{F}$ je ultrafilter, če in samo če za vsak $A \in \mathcal{P}(S)$ velja $A \in \mathcal{F}$ ali $S \setminus A \in \mathcal{F}$.
2. Če je $\mathcal{F}$ ultrafilter in $A_1 \cup \cdots \cup A_n \in \mathcal{F}$, potem je $A_i \in \mathcal{F}$ za nek i.
3. Če je $G \subseteq \mathcal{P}(S)$ z lastnostjo, da je vsak presek končno mnogo množic v G neprazen, potem je G vsebovan v nekem filtru.

Dokaz. Dokažimo le 1. točko, dokaz 2. in 3. točke je podobne zahtevnosti (→ vaje).

($\Leftarrow$): Če je $\mathcal{F}'$ filter z lastnostjo $\mathcal{F}' \supsetneq \mathcal{F}$, potem obstaja $A \subseteq S$, da je $A \in \mathcal{F}' \setminus \mathcal{F}$. Zato je po predpostavki $S \setminus A \in \mathcal{F}$, s tem pa velja $\varnothing = (S \setminus A) \cap A \in \mathcal{F}'$. Protislovje. Torej je $\mathcal{F}$ res maksimalen filter.

($\Rightarrow$): Naj za neko množico $A \subseteq S$ velja $A \notin \mathcal{F}$ in $S \setminus A \notin \mathcal{F}$. Naj bo $\mathcal{G} = \{B \subseteq S \mid \exists F \in \mathcal{F} \colon F \cap A \subseteq B\}$.



Jasno je $\mathcal{G} \supseteq \mathcal{F}$ in $A \in \mathcal{G} \setminus \mathcal{F}$. Dokažimo, da je $\mathcal{G}$ filter. To bo protislovje z maksimalnostjo filtra $\mathcal{F}$.

- Če je $\varnothing \in \mathcal{G}$, potem je $F \cap A = \varnothing$ za nek $F \in \mathcal{F}$. Od tod sledi $F \subseteq S \setminus A$, zato je $S \setminus A \in \mathcal{F}$. Protislovje. ✓✓
- Naj bosta $G_1, G_2 \in \mathcal{F}$. Potem je $F_1 \cap A \subseteq G_1$ in $F_2 \cap A \subseteq G_2$ za neka $F_1, F_2 \in \mathcal{F}$. Sledi $F_1 \cap F_2 \cap A \subseteq G_1 \cap G_2$ in $F_1 \cap F_2 \in \mathcal{F}$, zato je $G_1 \cap G_2 \in \mathcal{G}$. ✓✓
- Naj bo $G \in \mathcal{G}$ in $H \supseteq G$. Potem je $F \cap A \subseteq G \subseteq H$ za nek $F \in \mathcal{F}$, zato je $H \in \mathcal{G}$. ✓✓

□

Ultralimite

Izberimo nek neglavni ultrafilter $\mathcal{U}$ na množici $\mathbb{N}$. Naj bo T nek topološki prostor, v katerem opazujmo zaporedje $\{x_n\}_{n \in \mathbb{N}}$. Za $x \in T$ in okolico $x \in U \subseteq_o T$ označimo $I(U) = \{n \in \mathbb{N} \mid x_n \in U\}$. Točka x je $\mathcal{U}$-limita zaporedja

$\{x_n\}_{n\in\mathbb{N}}$, če za vsako odprto okolico U točke x velja $I(U)\in\mathcal{U}$.[24] V tem primeru pišemo $x=\lim_{\mathcal{U}} x_n$.

Zgled. Naj bo $\mathcal{F}$ kokončni filter. Tedaj je $x=\lim_{n\to\infty} x_n$, če in samo če je $x=\lim_{\mathcal{F}} x_n$.

Spomnimo se, da so neglavni ultrafiltri ravno ultrafiltri nad kokončnim filtrom in njihov presek je kokončni filter. Od tod izpeljemo, da limite vzdolž vseh neglavnih ultrafiltrov hkrati podajajo enako informacijo kot običajne limite.

Trditev. Velja $x=\lim_{n\to\infty} x_n$, če in samo če za vsak neglavni ultrafilter $\mathcal{U}$ na $\mathbb{N}$ velja $x=\lim_{\mathcal{U}} x_n$.

V tem smislu si lahko predstavljamo, da z ultrafiltrom $\mathcal{U}$ definiramo pojem $\mathcal{U}$-limite, ki je *bolj specifičen* od pojma običajne limite. V dovolj lepem topološkem prostoru T te specifične limite *vedno obstajajo* in so enolične.

Trditev.
1. Če je T Hausdorffov prostor, potem je $\mathcal{U}$-limita enolična.
2. Če je T kompakten, potem ima vsako zaporedje $\mathcal{U}$-limito.

Dokaz. 1. Naj bosta $x\neq y$ različni $\mathcal{U}$-limiti zaporedja $\{x_n\}_{n\in\mathbb{N}}$. Po predpostavki o Hausdorffovosti obstajata $U,V\subseteq_o T$, da velja $U\cap V=\emptyset$, $x\in U$, $y\in V$. Sledi $I(U)\cap I(V)=\emptyset$, zato množici $I(U),I(V)$ ne moreta obe pripadati $\mathcal{U}$. Protislovje.

2. Denimo, da zaporedje $\{x_n\}_{x\in\mathbb{N}}$ nima $\mathcal{U}$-limite. Torej ima vsak $y\in T$ odprto okolico $U_y\subseteq_o T$, da je $I(U_y)\notin\mathcal{U}$. Po predpostavki o kompaktnosti obstajajo $y_1,\ldots,y_k\in T$, da je $T=\bigcup_{i=1}^k U_{y_i}$. Hkrati za vsak i velja $I(U_{y_i})^c=\{n\in\mathbb{N}\mid x_n\notin U_{y_i}\}\in\mathcal{U}$, zato je $\bigcap_{i=1}^k I(U_{y_i})^c\in\mathcal{U}$. V posebnem je zadnji presek neprazen, torej obstaja $i_0\in\mathbb{N}$, da je $x_{i_0}\notin U_{y_i}$ za vsak i. Protislovje, saj množice U_{y_i} pokrijejo ves T. □

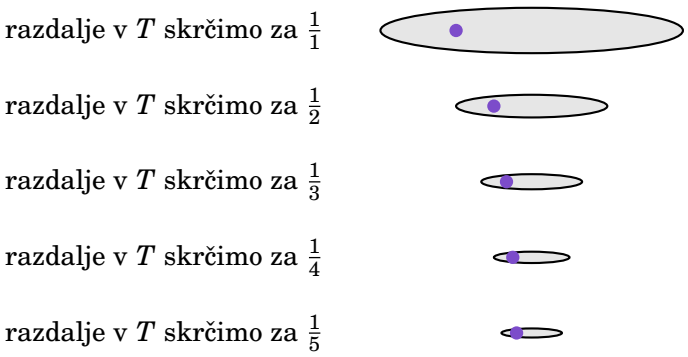
Zgled. Naj bo $\{x_n\}_{n\in\mathbb{N}}$ zaporedje v $[0,1]\subseteq\mathbb{R}$. Tedaj to zaporedje $\mathcal{U}$-konvergira za vsak neglavni ultrafilter $\mathcal{U}$ in ima enolično $\mathcal{U}$-limito.

Za *omejena zaporedja realnih števil* ima $\mathcal{U}$-limita običajne lastnosti limite. Lahko je preveriti linearnost in monotonost:

- $\lim_{\mathcal{U}}(x_n+y_n)=\lim_{\mathcal{U}} x_n+\lim_{\mathcal{U}} y_n$,
- $\lim_{\mathcal{U}}(c_n)=c\lim_{\mathcal{U}} x_n$,
- če je $x_n\leq y_n$ za vsak n, potem je $\lim_{\mathcal{U}} x_n\leq\lim_{\mathcal{U}} y_n$.

Trditev. Naj bo $\{x_n\}_{n\in\mathbb{N}}$ zaporedje v topološkem prostoru T. Naj bo $x\in T$. Predpostavimo, da T zadošča prvemu separacijskemu aksiomu T_1 in da je 1-števen. Tedaj je $x=\lim_{\mathcal{U}} x_n$ za nek neglavni ultrafilter $\mathcal{U}$, če in samo če je x (običajna) limita nekega podzaporedja $\{x_n\}_{n\in\mathbb{N}}$.

[24] Za vsako okolico U torej indeksi členov zaporedja, ki so v U, tvorijo *veliko* podmnožico $\mathbb{N}$. Pri tem smo bolj natančni kot pri običajni definiciji limite, kjer zahtevamo le, da so vsi razen končno mnogo členov zaporedja v U.



Slika 5.6: Zaporedje v T, ki ga opazujemo od daleč – razdalje v T na vsakem koraku skrčimo

Ultralimita torej *izbere* neko stekališče zaporedja.

Dokaz. ($\Rightarrow$): Naj bo $x = \lim_{\mathcal{U}} x_n$. Naj bo $\{U_i\}_{i\in\mathbb{N}}$ padajoča baza odprtih okolic točke x. Velja $I(U_1) \in \mathcal{U}$, zato je v posebnem $I(U_1) \neq \emptyset$, torej obstaja $n_1 \in \mathbb{N}$, da je $x_{n_1} \in U_1$. Ker ultrafilter $\mathcal{U}$ vsebuje kokončni filter, induktivno za vsak $i > 1$ velja $I(U_i) \cap \{1,2,\ldots,n_{i-1}\}^c \in \mathcal{U}$, zato obstaja $n_i \in \mathbb{N}$, da je $n_i > n_{i-1}$ in $x_{n_i} \in U_i$. Torej je $\lim_{i\to\infty} x_{n_i} = x$. ✓✓

($\Leftarrow$): Naj bo x stekališče zaporedja $\{x_n\}_{n\in\mathbb{N}}$. Naj bo $\{U_i\}_{i\in\mathbb{N}}$ padajoča baza odprtih okolic točke x. Ker je x stekališče, je $I(U_1) \neq \emptyset$, torej obstaja $n_1 \in \mathbb{N}$, da je $x_{n_1} \in U_1$. Induktivno za vsak $i > 1$ obstaja $n_i \in \mathbb{N}$, da je $x_{n_i} \in U_i$ in $n_i > n_{i-1}$. Naj bo $G = \{I(U_i)\setminus\{1,2,\ldots,n_{i-1}\} \mid i \in \mathbb{N}\}$. Uporabimo (OSNOVNE LASTNOSTI ULTRAFILTROV) in sklepamo, da obstaja ultrafilter $\mathcal{U} \supseteq G$. S tem je $x = \lim_{\mathcal{U}} x_n$. Hkrati ultrafilter $\mathcal{U}$ ni glavni, saj za vsak $k \in \mathbb{N}$ za dovolj velik i velja $k \notin I(U_i)\setminus\{1,2,\ldots,n_{i-1}\}$. □

Asimptotski stožec

Fiksirajmo neglavni ultrafilter $\mathcal{U}$ na $\mathbb{N}$. Opazujmo metrični prostor T z odlikovano točko $e \in T$.[25] Asimptotski stožec prostora T bomo konstruirali podobno kot konstruiramo $\mathbb{R}$ iz $\mathbb{Q}$: realna števila so Cauchyjeva zaporedja racionalnih števil modulo zaporedja z limito 0. Pri tem bomo iz tehničnih razlogov obravnavali le *posebna* zaporedja v T.

Zaporedje zmerne rasti je zaporedje $\{x_n\}_{n\in\mathbb{N}}$ v T, ki zadošča pogoju

$$\forall n \in \mathbb{N}: \quad d(x_n, e) \leq An$$

za neko konstanto A, odvisno le od zaporedja $\{x_n\}_{n\in\mathbb{N}}$.[26] Razdalja med zaporedjema zmerne rasti $\alpha = \{x_n\}_{n\in\mathbb{N}}$ in $\beta = \{y_n\}_{n\in\mathbb{N}}$ je

$$d(\alpha,\beta) = \lim_{\mathcal{U}} \left(\frac{d(x_n, y_n)}{n} \right).$$[27]

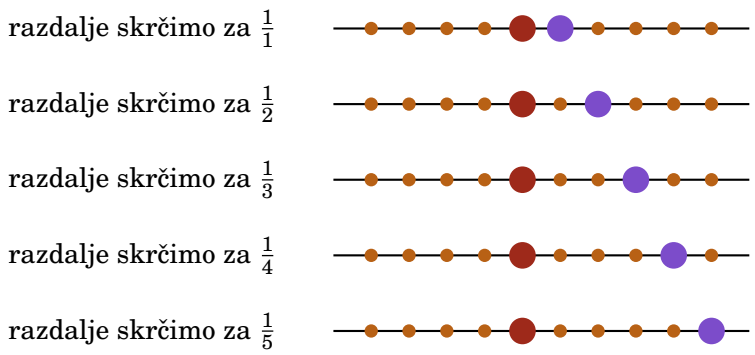
Zgled. Naj bo $T = \mathrm{Cay}(\mathbb{Z}, \{1\})$.

Izberimo najprej $\alpha = \{0\}_{n\in\mathbb{N}}$ in $\beta = \{1\}_{n\in\mathbb{N}}$. Velja $d(0,1)/n = 1/n$ za vsak n, zato je $d(\alpha,\beta) = \lim_{\mathcal{U}} 1/n = 0$. V asimptotskem stožcu bomo ti dve zaporedji torej identificirali.

[25] Nas bo nazadnje zanimal primer, ko je $T = \mathrm{Cay}(G,S)$ in $e = 1 \in G$.

[26] Z drugimi besedami, zaporedje zmerne rasti pomeni, da je $\limsup_{n\to\infty} d(x_n,e)/n < \infty$.

[27] Pri tem je $d(x_n,y_n) \leq d(x_n,e) + d(e,y_n) \leq Cn$ za neko konstanto C, zato je zaporedje $\{d(x_n,y_n)/n\}_{n\in\mathbb{N}}$ omejeno, torej za njegovo $\mathcal{U}$-limito veljajo običajne lastnosti limite.



Slika 5.7: Razdalja med zaporedjema $\{0\}_{n\in\mathbb{N}}$ in $\{n\}_{n\in\mathbb{N}}$ v grafu $\mathrm{Cay}(\mathbb{Z},\{1\})$, ki ga opazujemo od daleč, je enaka 1

Izberimo zdaj $\alpha=\{0\}_{n\in\mathbb{N}}$ in $\beta=\{n\}_{n\in\mathbb{N}}$. Velja $d(0,n)/n=1$ za vsak n, zato je $d(\alpha,\beta)=1$. V asimptotskem stožcu bo torej zaporedje α predstavljalo število $0\in\mathbb{R}$, zaporedje β pa število $1\in\mathbb{R}$.

Recimo, da sta zaporedji α,β ekvivalentni, če velja $d(\alpha,\beta)=0$. Množica vseh ekvivalenčnih razredov zaporedij zmerne rasti se imenuje asimptotski stožec prostora T z odlikovano točko e glede na $\mathcal{U}$, oznaka $\mathrm{Cone}_{\mathcal{U}}(T,e)$. Razdalja d na zaporedjih se prenese na stožec, zato je $\mathrm{Cone}_{\mathcal{U}}(T,e)$ *metrični prostor*.

Zgled.

- Naj bo $T=\mathbb{R}$. Ta prostor se ne spremeni s krčenjem razdalj, zato pričakujemo, da je $\mathrm{Cone}_{\mathcal{U}}(\mathbb{R},0)$ izometričen $\mathbb{R}$. Pričakovanje potrdita inverzni izometriji

  $$f:\mathbb{R}\to\mathrm{Cone}_{\mathcal{U}}(\mathbb{R},0),\quad x\mapsto[\{nx\}_{n\in\mathbb{N}}]$$

  in

  $$g:\mathrm{Cone}_{\mathcal{U}}(\mathbb{R},0)\to\mathbb{R},\quad [\{x_n\}_{n\in\mathbb{N}}]\to d(\{x_n\}_{n\in\mathbb{N}},\{0\}_{n\in\mathbb{N}})=\lim_{\mathcal{U}}\left(\frac{x_n}{n}\right).$$

- Naj bo $T=\mathbb{Z}$, opremljen z metriko iz $\mathrm{Cay}(\mathbb{Z},\{1\})$. Trdimo, da je $\mathrm{Cone}_{\mathcal{U}}(\mathbb{Z},0)$ izometričen $\mathbb{R}$. Definirajmo preslikavi

  $$f:\mathbb{R}\to\mathrm{Cone}_{\mathcal{U}}(\mathbb{Z},0),\quad x\mapsto[\{\lfloor nx_n\rfloor\}_{n\in\mathbb{N}}]$$

  in

  $$g:\mathrm{Cone}_{\mathcal{U}}(\mathbb{Z},0)\to\mathbb{R},\quad [\{x_n\}_{n\in\mathbb{N}}]\mapsto d(\{x_n\}_{n\in\mathbb{N}},\{0\}_{n\in\mathbb{N}})=\lim_{\mathcal{U}}\left(\frac{x_n}{n}\right).$$

  Preprosto je preveriti, da f in g ohranjata razdalji na obeh metričnih prostorih. Preverimo, da sta ti dve preslikavi inverzni. Za zaporedje zmerne rasti $\{x_n\}_{n\in\mathbb{N}}$ velja

  $$(f\circ g)([\{x_n\}_{n\in\mathbb{N}}])=[\{\lfloor\lim_{\mathcal{U}}\frac{x_n}{n}\cdot m\rfloor\}_{m\in\mathbb{N}}]=[\{\lfloor\lim_{\mathcal{U}}(x_n\frac{m}{n})\rfloor\}_{m\in\mathbb{N}}].$$

  Preverimo, da je zadnji ekvivalenčni razred enak $[\{x_m\}_{m\in\mathbb{N}}]$. V ta namen izračunajmo razdaljo med njima. Velja

  $$\begin{aligned}d\left(\{\lfloor\lim_{\mathcal{U}}(x_n\frac{m}{n})\rfloor\}_{m\in\mathbb{N}},\{x_m\}_{m\in\mathbb{N}}\right)&=\lim_{\mathcal{U}}\frac{1}{m}\cdot d\left(\lfloor\lim_{\mathcal{U}}(x_n\frac{m}{n})\rfloor,x_m\right)\\&=\lim_{\mathcal{U}}\frac{1}{m}\cdot|\lfloor\lim_{\mathcal{U}}(x_n\frac{m}{n})\rfloor-x_m|\\&=|\lim_{\mathcal{U}}\frac{x_n}{n}-\lim_{\mathcal{U}}\frac{x_m}{m}|=0,\end{aligned}$$

kjer smo v predzadnji enakosti uporabili $\lim_{m\to\infty}\frac{1}{m}\lfloor cm\rfloor = c$ za vsak $c\in\mathbb{R}$. Torej je res $f\circ g = \mathrm{id}_{\mathrm{Cone}_{\mathcal{U}}(\mathbb{Z},0)}$. Druga enakost, $g\circ f = \mathrm{id}_{\mathbb{R}}$, sledi neposredno iz $\lim_{m\to\infty}\frac{1}{m}\lfloor cm\rfloor = c$.

Asimptotski stožec grupe

Naj bo G končno generirana grupa, $G=\langle S\rangle$. Opazujmo Cayleyjev graf $\mathrm{Cay}(G,S)$, opremljen z metriko $d(x,y)=\ell_S(x^{-1}y)$. Za odlikovano točko vzemimo $1\in G$. Dobimo asimptotski stožec $K=\mathrm{Cone}_{\mathcal{U}}(\mathrm{Cay}(G,S),1)$. Množico vseh zaporedij zmerne rasti označimo z ZZR. Množica ZZR je grupa z enoto $1=\{1\}_{n\in\mathbb{N}}$. Naj bo ZZR_0 množica tistih zaporedij $\alpha\in\mathrm{ZZR}$, za katera je $d(\alpha,1)=0$. Množica ZZR_0 je podgrupa ZZR. Asimptotski stožec K lahko zato identificiramo z množico odsekov $\mathrm{ZZR}/\mathrm{ZZR}_0$.

V primeru konstrukcije iz grup ima asimptotski stožec veliko dobrih topoloških lastnosti.

Trditev. Asimptotski stožec K grupe G je homogen, lokalno povezan, s potmi povezan in poln metrični prostor.

Dokaz. Homogenost: Asimptotski stožec identificiramo z množico odsekov $\mathrm{ZZR}/\mathrm{ZZR}_0$. Na tej množici deluje grupa ZZR z levim množenjem: $\{z_n\}_{n\in\mathbb{N}}.\{x_n\}_{n\in\mathbb{N}}\mathrm{ZZR}_0=\{z_n\cdot x_n\}_{n\in\mathbb{N}}\mathrm{ZZR}_0$. To delovanje je tranzitivno, saj je $\{y_nx_n^{-1}\}_{n\in\mathbb{N}}.\{x_n\}_{n\in\mathbb{N}}\mathrm{ZZR}_0=\{y_n\}_{n\in\mathbb{N}}\mathrm{ZZR}_0$. ✓

Povezanost s potmi:

Za vsak $\alpha\in K$ obstaja zvezna pot $\gamma\colon[0,1]\to K$ z $\gamma(0)=1$ in $\gamma(1)=\alpha$.

Dokaz: Naj bo $\alpha=[\{x_n\}_{n\in\mathbb{N}}]$. Vsak člen x_n zapišimo kot besedo dolžine $\ell_S(x_n)$, torej $x_n=s_1s_2\cdots s_{\ell_S(x_n)}$. Naj bo $0\le t\le 1$ parameter in naj $x_n(t)$ označi predpono izbrane besede za x_n dolžine $\lfloor t\cdot\ell_S(x_n)\rfloor$, se pravi $x_n(t)=s_1s_2\cdots s_{\lfloor t\cdot\ell_S(x_n)\rfloor}$. Definirajmo $\gamma(t)=[\{x_n(t)\}_{n\in\mathbb{N}}]\in K$. Jasno je $\gamma(0)=1$ in $\gamma(1)=\alpha$. Za vsaka $t_1<t_2$ velja

$$\begin{aligned} d(x_n(t_1),x_n(t_2)) &= \big|\lfloor t_2\cdot\ell_S(x_n)\rfloor-\lfloor t_1\cdot\ell_S(x_n)\rfloor\big| \\ &\le (t_2-t_1)\cdot\ell_S(x_n)+1. \end{aligned}$$

Od tod sledi

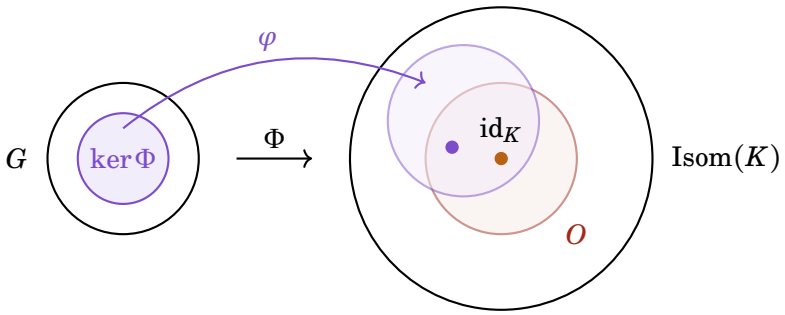
$$d(\gamma(t_1),\gamma(t_2))=\lim_{\mathcal{U}}\frac{d(x_n(t_1),x_n(t_2))}{n}\le d(\alpha,1)\cdot(t_2-t_1).$$

Preslikava γ je torej Lipschitzovo zvezna. ✓

Lokalna povezanost: Naj bo $\alpha=[\{x_n\}_{n\in\mathbb{N}}]\in K$ in naj bo γ pot kot v pomožni trditvi. Po konstrukciji za vsak $t\in[0,1]$ velja $d(\gamma(t),1)\le d(\alpha,1)\cdot t$, zato je slika γ v celoti vsebovana v krogli $B_K(d(\alpha,1))$[28]. Iz pomožne trditve zato sledi, da je notranjost krogle $B_K(d(\alpha,1))$ povezana. Ker je prostor K homogen, od tod sledi lokalna povezanost prostora K. ✓

Polnost: (→ vaje) □

[28] $B_K(r)$ je krogla polmera r v metričnem prostoru K s središčem $1=[\{1\}_{n\in\mathbb{N}}]\in K$.



Slika 5.8: Za vsako okolico O identitete $\mathrm{id}_K \in \mathrm{Isom}(K)$ obstaja homomorfizem $\varphi\colon \ker\Phi \to \mathrm{Isom}(K)$, katerega slika vsebuje vsaj en netrivialen element v O

Delovanje grupe na asimptotskem stožcu

Naj bo G grupa in $K = \mathrm{Cone}_{\mathcal{U}}(\mathrm{Cay}(G,S),1)$ njen asimptotski stožec. Grupa G naravno deluje z levo translacijo na zaporedjih v G:

$$g.\{x_n\}_{x\in\mathbb{N}} = \{gx_n\}_{n\in\mathbb{N}} \quad \text{za } g, x_n \in G.$$

Če je zaporedje $\{x_n\}_{x\in\mathbb{N}}$ zmerne rasti, je pri tem tudi $g.\{x_n\}_{x\in\mathbb{N}}$ zmerne rasti.[29] Ker G deluje z izometrijami na $\mathrm{Cay}(G,S)$, velja tudi

$$d(g.\{x_n\}_{n\in\mathbb{N}}, g.\{y_n\}_{n\in\mathbb{N}}) = d(\{x_n\}_{n\in\mathbb{N}}, \{y_n\}_{n\in\mathbb{N}}).$$

Tako G deluje z izometrijami na grupi zmernih zaporedij ZZR in zato deluje tudi na kvocientni množici odsekov $\mathrm{ZZR}/\mathrm{ZZR}_0 \equiv K$. Dobimo torej homomorfizem

$$\Phi\colon G \to \mathrm{Isom}(K), \quad g \mapsto ([\{x_n\}_{x\in\mathbb{N}}] \mapsto [\{gx_n\}_{x\in\mathbb{N}}]).$$

Grupa izometrij $\mathrm{Isom}(K)$ je *topološka grupa*: opremljena je s topologijo, pri kateri baza okolic izometrije id_K sestoji iz množic

$$O_{k,\epsilon} = \{\sigma \in \mathrm{Isom}(K) \mid d(\sigma.a, a) < \epsilon \text{ za vsak } a \in B_K(k)\}$$

za $k \in \mathbb{N}$ in $\epsilon > 0$. To je topologija enakomerne konvergence po kompaktih.

Pri dokazu izreka Gromova bomo ključno uporabili naslednjo lastnost delovanja G na K.[30]

Izrek. (O DELOVANJU Φ) Predpostavimo, da je slika $\mathrm{im}\,\Phi$ končna in da jedro $\ker\Phi$ *ni* virtualno abelova grupa. Tedaj za vsako okolico O identitete $\mathrm{id}_K \in \mathrm{Isom}(K)$ obstaja homomorfizem $\varphi\colon \ker\Phi \to \mathrm{Isom}(K)$ z lastnostjo $|\mathrm{im}\,\varphi \cap O| > 1$.

Dokaz. Za $g \in G$ in $r \in \mathbb{R}$ označimo največji možni premik[31] elementa g na krogli polmera r kot

$$D(g,r) = \max\{d(a, g\cdot a) \mid a \in B_{G,S}(r)\} = \max\{\ell_S(a^{-1}ga) \mid a \in B_{G,S}(r)\}.$$

Za vsaka $g \in \ker\Phi$ in $C > 0$ velja $\lim_{\mathcal{U}} \frac{D(g,Cr)}{r} = 0$.

[29] Za vsak n velja $d(gx_n, 1) = \ell_S(gx_n) \le \ell_S(x_n) + \ell_S(g) \le Cn$ za neko konstanto C.
[30] Dokaz je *precej* zahteven.
[31] Angleško *displacement*.

Dokaz: Za vsak $r \in \mathbb{N}$ izberimo $a_r \in B_{G,S}(Cr)$ z lastnostjo $D(g,Cr) = \ell_S(a_r^{-1} g a_r)$. Zaporedje $\alpha = \{a_r\}_{r\in\mathbb{N}}$ je zmerne rasti. Ker je $g \in \ker\Phi$, velja $g.[\alpha] = [\alpha]$, se pravi $d(g.[\alpha],[\alpha]) = 0$, kar je ekvivalentno

$$\lim_{\mathcal{U}} \frac{D(g,Cr)}{r} = \lim_{\mathcal{U}} \frac{d(ga_r,a_r)}{r} = 0.$$

Dokaz je zaključen. ✓✓

Za fiksen $g \in G$ je funkcija $D(g,\cdot):\mathbb{N}\to\mathbb{R}$ omejena, če in samo če je $|g^G| < \infty$. V tem primeru velja $g \in \ker\Phi$.

Dokaz: Očitno iz definicije D in zadnjega dokaza. ✓✓

Elementi $g \in G$ z lastnostjo $|g^G| < \infty$ se imenujejo FC-elementi.[32] Ti elementi tvorijo podgrupo edinko v G.

Za vse $g,h \in G$ in $r,s \in \mathbb{Z}$ velja:
1. $D(g,r+s) \le D(g,r) + 2s$
2. $D(h^{-1}gh,r) \le D(g,r) + 2\ell_S(h)$

Dokaz: 1. Naj bo $a \in B_{G,S}(r+s)$. Zapišimo $a = b\cdot c$ za neka $b \in B_{G,S}(r)$ in $c \in B_{G,S}(s)$. Tedaj je

$$\begin{aligned} d(ga,a) = d(gbc,bc) &\le d(gbc,gb) + d(gb,b) + d(b,bc) \\ &= \ell_S(c) + d(gb,b) + \ell_S(c) \\ &\le D(g,r) + 2s, \end{aligned}$$

kar smo želeli dokazati. ✓✓

2. Naj bo $a \in B_{G,S}(r)$. Velja

$$d(h^{-1}gha,a) = d(gha,ha) \le D(g,r+\ell_S(h)) \le D(g,r) + 2\ell_S(h),$$

kjer smo v zadnji neenakosti uporabili prejšnjo točko. ✓✓

Nobena grupa *ni* končna unija odsekov pogrup neskončnega indeksa.

Dokaz: Elementarno. (→ vaje)✓✓

Z vsem naštetim lahko nazadnje dokažemo izrek (O DELOVANJU Φ). Po predpostavki je $|\operatorname{im}\Phi| = |G : \ker\Phi| < \infty$. Torej je jedro $\ker\Phi$ končno generirana grupa, označimo $\ker\Phi = \langle y_1,\dots,y_d\rangle$. Naj bo $O_{C',\epsilon'} \subseteq \operatorname{Isom}(K)$ poljubna bazna okolica identitete id_K in naj bo $C = 2C'$, $\epsilon = \epsilon'/2$. Dokaz bomo izvedli v zaporedju večih korakov.

- Predpostavimo najprej, da je vsak generator y_j FC-element. V tem primeru je $|y_j^{\ker\Phi}| < \infty$, zato je centralizator $C_{\ker\Phi}(y_j)$ končnega indeksa v $\ker\Phi$ za vsak j. Od tod sledi, da je tudi $Z(\ker\Phi) = \bigcap_{j=1}^{d} C_{\ker\Phi}(y_j)$ končnega indeksa v $\ker\Phi$. To pomeni, da je grupa $\ker\Phi$ virtualno abelova. Protislovje. Torej FC-elementi tvorijo pravo podgrupo v $\ker\Phi$, zato lahko po morebitni menjavi generatorjev grupe $\ker\Phi$ predpostavimo, da celo

  noben od y_j ni FC-element.[33]

[32] Iz angleškega izraza *finitely many conjugates*.

[33] Če y_{j_0} ni FC-element in y_j je FC-element, potem lahko y_j zamenjamo z $y_j y_{j_0}$, ki ni FC-element.

- Fiksirajmo $r \in \mathbb{N}$. Opazujmo množico

$$\begin{aligned} Y_t &= \{y \in \ker\Phi \mid D(y^{-1}y_t y, Cr) \le \epsilon r\} \\ &= \{y \in \ker\Phi \mid \forall a \in B_{G,S}(Cr)\colon\ \ell_S(a^{-1}y^{-1}y_t y a) \le \epsilon r\} \\ &= \{y \in \ker\Phi \mid \forall a \in B_{G,S}(Cr)\colon\ y_t^{ya} \in B_{G,S}(\epsilon r)\}. \end{aligned}$$

  Množica $\{y_t^{ya} \mid y \in Y_t,\ a \in B_{G,S}(Cr)\}$ je torej končna, saj je vsebovana v $B_{G,S}(\epsilon r)$. Zato je tudi množica odsekov $C_t = \{C_{\ker\Phi}(y_t)ya \mid y \in Y_t,\ a \in B_{G,S}(Cr)\}$ končna. Ker y_t ni FC-element, je vsak centralizator $C_{\ker\Phi}(y_t)$ neskončnega indeksa v $\ker\Phi$, zato po zadnji pomožni trditvi $\ker\Phi$ ni unija odsekov iz $C_1 \cup \cdots \cup C_d$. Tako obstaja element $z_r \in \ker\Phi$, ki ne pripada nobenemu odseku iz C_t. V posebnem od tod sledi, da za vsak t velja $z_r \notin Y_t$, se pravi

$$\text{za vsak } t \text{ velja } D(z_r^{-1}y_t z_r, Cr) > \epsilon r.$$

- Zapišimo element z_r kot besedo v $y_1, \ldots, y_d$ in naj bo x_r najkrajša predpona besede, za katero za *nek* t velja $D(x_r^{-1}y_t x_r, Cr) > \epsilon r$. Izberimo en tak $t = t(r)$.[34] Za vsak $i = 1, \ldots, d$ naj bo $S(i) = \{r \mid t(r) = i\}$. Velja $S(1) \cup \cdots \cup S(d) = \mathbb{N}$. Torej obstaja i_0, da je $S(i_0) \in \mathcal{U}$. Torej velja

$$D(x_r^{-1}y_{i_0}x_r, Cr) > \epsilon r \text{ za vse } r \text{ iz neke množice v } \mathcal{U}.$$

- Po prvi pomožni trditvi za vse r iz neke množice v $\mathcal{U}$ velja $D(y_t, r) < \epsilon r$ za vsak t. Od tod sledi, da je $x_r \neq 1$, torej lahko pišemo $x_r = w_r \cdot y$ za nek $y \in \{y_1^{\pm 1}, \ldots, y_d^{\pm 1}\}$ in krajšo besedo w_r. Iz tretje pomožne trditve zdaj sledi

$$D(x_r^{-1}y_t x_r, Cr) = D(y^{-1}w_r^{-1}y_t w_r y, Cr) \le D(w_r^{-1}y_t w_r, Cr) + 2\ell_S(y).$$

  Naj bo $\ell = \max\{\ell_S(y_i) \mid i = 1, \ldots, d\}$. Torej

  za vse r iz neke množice v $\mathcal{U}$ je $D(x_r^{-1}y_t x_r, Cr) \le \epsilon r$[35] $+ 2\ell$ za vsak t.

- Za vse r iz neke množice v $\mathcal{U}$ torej velja neenakost

$$\epsilon r < D(x_r^{-1}y_{i_0}y_r, Cr) \le \epsilon r + 2\ell,$$

  od koder sledi

$$\lim_{\mathcal{U}} \frac{D(x_r^{-1}y_{i_0}x_r, Cr)}{r} = \epsilon. \tag{5.1}$$

- Za poljuben element $w \in \ker\Phi$ opazujmo zaporedje $\{x_r^{-1}wx_r\}_{r\in\mathbb{N}}$ v grupi G. Zapišimo w kot besedo v generatorjih $y_1, \ldots, y_d$ dolžine m. Velja

$$\ell_S(x_r^{-1}wx_r) \le D(x_r^{-1}wx_r, Cr) \le m \cdot \max\{D(x_r^{-1}y_i x_r, Cr) \mid i = 1, \ldots, d\}.$$

  Za vse r iz neke množice $U \in \mathcal{U}$ zato velja

$$\ell_S(x_r^{-1}wx_r) \le m\epsilon r + 2m\ell.$$

[34] Velja torej $D(x_r^{-1}y_{t(r)}x_r, Cr) > \epsilon r$.

[35] Tu smo upoštevali minimalnost dolžine elementa x_r, od koder sledi $D(w_r^{-1}y_t w_r, Cr) \le \epsilon r$ za vsak t.

Definirajmo zaporedje $\{X_r(w)\}_{r\in\mathbb{N}}$ na naslednji način:

$$X_r(w) = \begin{cases} x_r^{-1} w x_r; & r \in U \\ 1; & r \in \mathbb{N}\backslash U. \end{cases}$$

Zaporedji, ki se na množici v $\mathcal{U}$ ujemata, imata enako $\mathcal{U}$-limito, zato velja

$$d(\{X_r(w)\}_{r\in\mathbb{N}}, \{x_r^{-1} w x_r\}_{r\in\mathbb{N}}) = 0 \quad \text{in} \quad \{X_r(w)\}_{r\in\mathbb{N}} \in \mathrm{ZZR}.$$

- Zaporedje zmerne rasti $\{X_r(w)\}_{r\in\mathbb{N}}$ lahko z desne pomnožimo z drugimi zmernimi zaporedji in na ta način dobimo izometrijo asimptotskega stožca $\mathrm{ZZR}/\mathrm{ZZR}_0 = K$. To izometrijo označimo s $\varphi(w)$. Imamo torej homomorfizem grup

$$\varphi : \ker \Phi \to \mathrm{Isom}(K).$$

- Kot v dokazu prve pomožne trditve zdaj iz lastnosti (5.1) sledi, da zaporedje $\{X_r(y_{i_0})\}_{r\in\mathbb{N}}$ deluje netrivialno z levim množenjem na K. Torej je $\varphi(y_{i_0}) \neq \mathrm{id}_K$.

- Naj bo $\alpha = \{a_r\}_{r\in\mathbb{N}} \in \mathrm{ZZR}$ z $[\alpha] \in B_K(C/2)$. Za vse r iz neke množice v $\mathcal{U}$ velja torej $a_r \in B_{G,S}(Cr)$. Od tod sledi

$$\begin{aligned} d(\varphi(y_{i_0}).[\alpha], [\alpha]) &= d(\{X_r(y_{i_0})\}_{r\in\mathbb{N}}, \{a_r\}_{r\in\mathbb{N}}) \\ &= \lim_{\mathcal{U}} \frac{d(X_r(y_{i_0})a_r, a_r)}{r} \\ &\leq \lim_{\mathcal{U}} \frac{D(X_r(y_{i_0}), Cr)}{r} \\ &= \lim_{\mathcal{U}} \frac{D(x_r^{-1} y_{i_0} x_r, Cr)}{r} \\ &= \epsilon. \end{aligned}$$

Torej je $\varphi(y_{i_0}) \in O_{C/2,2\epsilon} = O_{C',\epsilon'}$. S tem je dokaz zaključen. □

5.5 Izrek Gromova

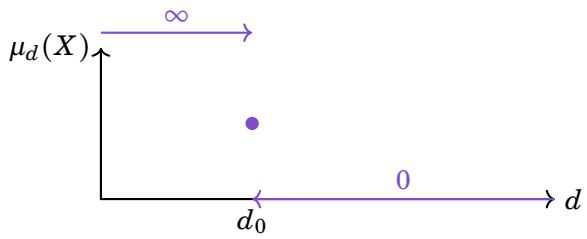
V tem razdelku bomo končno dokazali izrek Gromova.

Izrek. (Gromov 1981) Grupe polinomske rasti so virtualno nilpotentne.

Hausdorffova dimenzija

Naš prvi cilj je, da dokažemo, da je asimptotski stožec grupe polinomske rasti končno dimenzionalen. V ta namen bomo dokazali nekoliko močnejšo trditev, v kateri bomo *merili dimenzijo* s pokrivanjem objekta s kroglami.

Zgled. Opazujmo *dovolj lepo* podmnožico v $\mathbb{R}^n$. Njen volumen lahko izračunamo tako, da jo pokrijemo s kroglami polmera ϵ, seštejemo volumne krogel in pošljemo ϵ proti 0. Volumen krogle polmera ϵ v $\mathbb{R}^n$ je $\frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)} \cdot \epsilon^n$, kjer je Γ Eulerjeva funkcija. Če odmislimo prvi faktor, potem vsaka krogla



Slika 5.9: Hausdorffova mera $\mu_d(X)$ za različne vrednosti d

prispeva k vsoti člen ϵ^n. Pri tem je ϵ polmer krogle, n pa dimenzija prostora $\mathbb{R}^n$.

Naj bo M metrični prostor in $X \subseteq M$. Opazujmo vsa *števna* pokritja množice X z množicami premera $< \epsilon$ za nek ϵ. Za vsako tako pokritje $\{U_i\}_i$ izračunamo $\sum_i (\operatorname{diam} U_i)^d$ za nek fiksen $d > 0$. Izlimitiramo $\epsilon \to 0$ in dobimo

$$\mu_d(X) = \lim_{\epsilon \to 0} \inf_{\{U_i\}_i \text{ pokritje } X \text{ z } \operatorname{diam} U_i < \epsilon} \sum_i (\operatorname{diam} U_i)^d,$$

to je d-dimenzionalna Hausdorffova mera množice X. Bolj kot mera sama nas zanima, kakšne so njene vrednosti, ko se d spreminja. Po motivaciji iz evklidskih prostorov pričakujemo, da *pravilen volumen* izračunamo ravno z mero μ_d, kjer je d dimenzija prostora X.

Zgled. Naj bo $X = [0,1] \subseteq \mathbb{R}$. Velja:

- $\mu_1([0,1]) = 1$,
- $\mu_2([0,1]) \leq \lim_{n \to \infty, \epsilon := \frac{1}{n}} \sum_{i=1}^n \left(\frac{1}{n}\right)^2 = \lim_{n \to \infty} \frac{1}{n} = 0$,
- $\mu_{\frac{1}{2}}([0,1]) = \lim_{n \to \infty} \sum_{i=1}^n \frac{1}{n^{1/2}} = \infty$.

Dimenzija prostora $[0,1]$ je 1. Pravilen volumen smo izračunali z uporabo μ_1. Pri μ_2 in $\mu_{\frac{1}{2}}$ smo izračunalni nesmiselna volumna, 0 in ∞.

Ni težko premisliti (→ vaje), da kot v zadnjem zgledu za vsak X obstaja število $d_0 \in \mathbb{R}_{\geq 0} \cup \{\infty\}$, tako da je

$$\mu_d(X) = \begin{cases} \infty; & d < d_0 \\ m_0; & d = d_0 \\ 0; & d > d_0 \end{cases}$$

za nek $m_0 \in \mathbb{R}_{\geq 0} \cup \{\infty\}$.

Bolj kot mera m_0 nas zanima število d_0, ki ga imenujemo Hausdorffova dimenzija množice X, oznaka $\dim_H(X)$. Velja torej

$$d_0 = \dim_H(X) = \inf\{d \geq 0 \mid \mu_d(X) = 0\}.$$

Hausdorffova dimenzija ni nujno celo število.

Zgled.

- Hausdorffova dimenzija števnega metričnega prostora z diskretno topologijo je enaka 0.

- Opremimo množico $\mathbb{R}$ z diskretno metriko, kjer je razdalja med vsakima različnima številoma enaka 1. Odprta množica premera manj kot 1 vsebuje le eno točko. Števnih pokritij $\mathbb{R}$ z množicami takega premera torej ni in zato je Hausdorffova dimenzija v tem primeru enaka $\inf \varnothing = \infty$.

- Naj bo $C \subseteq [0,1]$ Cantorjeva množica, konstruirana kot presek $\bigcap_{k=1}^{\infty} C_k$, kjer je C_k unija 2^k intervalov dolžine $\frac{1}{3^k}$. Vsaka množica C_k nam torej podaja odprto pokritje množice C s podmnožicami premera $\frac{1}{3^k}$. Ko gre k čez vse meje, dobimo oceno za Hausdorffovo mero množice C:

$$\mu_d(C) \leq \lim_{k\to\infty} 2^k \cdot \left(\frac{1}{3^k}\right)^d = \lim_{k\to\infty} \left(\frac{2}{3^d}\right)^k.$$

  Če je $2 < 3^d$, se pravi $d > \frac{\log 2}{\log 3}$, je torej $\mu_d(C) = 0$. Od tod sledi $\dim_H(C) \leq \frac{\log 2}{\log 3} \approx 0.63$. Dokazati je mogoče, da velja celo enakost $\dim_H(C) = \frac{\log 2}{\log 3}$.

Hausdorffova dimenzija je definirana za metrične prostore, običajna topološka dimenzija pa je definirana za vse topološke prostore. Za dan metrični prostor lahko obstaja kak homeomorfen prostor, ki je tudi metrični, a ima drugačno Hausdorffovo dimenzijo. Najmanjša možna Hausdorffova dimenzija homeomorfnih modelov prostora je ravno topološka dimenzija.

Izrek. (Szpilrajn 1937) Naj bo X metrični prostor. Tedaj je topološka dimenzija X enaka najmanjši možni Hausdorffovi dimenziji $\dim_H(Y)$, kjer Y preteče metrične prostore, homeomorfne X.

Dokaz. Podajmo le idejo dokaza, da je topološka dimenzija prostora X vselej manjša ali enaka Hausdorffovi dimenziji.[36] Ekvivalentno, če je X topološki prostor z $\mu_{d+1}(X) = 0$, potem je X dimenzije kvečjemu d. Dokazujemo z indukcijo na d.

Naj bo $x \in X$ poljubna točka. Za vsak $r > 0$ opazujmo rob krogle okoli x, se pravi sfero $S(r) \subseteq X$ s središčem v x in polmerom r. Dovolj bo dokazati, da za nek r velja $\mu_d(S(r)) = 0$, izrek od tod sledi induktivno.

Za vsako podmnožico $A \subseteq X$ velja

$$\int_0^{\infty} \operatorname{diam}(S(r) \cap A)^d \, dr \leq \operatorname{diam}(A)^{d+1}.$$

Dokaz: Naj bo $r_1 = \inf_{a\in A} d(a,x)$ in $r_2 = \sup_{a\in A} d(a,x)$. Velja $r_2 - r_1 \leq \operatorname{diam}(A)$, od koder sledi

$$\begin{aligned}\int_0^{\infty} \operatorname{diam}(S(r) \cap A)^d \, dr &= \int_{r_1}^{r_2} \operatorname{diam}(S(r) \cap A)^d \, dr \\ &\leq \operatorname{diam}(A)^d \int_{r_1}^{r_2} dr \leq \operatorname{diam}(A)^{d+1}.\end{aligned}$$

[36] V nadaljevanju bomo uporabili le to lastnost dimenzij, saj bomo z uporabo Hausdorffove dimenzije dokazali, da je asimptotski stožec končne dimenzije.

Ker velja $\mu_{d+1}(X) = 0$, obstaja zaporedje števnih pokritij $\{U_i^n\}_i$ množice X za $n = 1, 2, \ldots$, tako da je

$$\lim_{n\to\infty} \sum_i \operatorname{diam}(U_i^n)^{d+1} = 0.$$

Iz pomožne trditve zdaj sledi

$$\lim_{n\to\infty} \int_0^\infty \sum_i \operatorname{diam}(S(r) \cap U_i^n)^d \, dr = 0.$$

Torej obstaja podzaporedje[37] zaporedja pokritij $\{U_i^{n_k}\}_i$ za $k = 1, 2, \ldots$, da za nek[38] $r > 0$ velja

$$\lim_{k\to\infty} \sum_i \operatorname{diam}(S(r) \cap U_i^{n_k})^d = 0.$$

Od tod sledi $\mu_d(S(r)) = 0$. □

Končno dimenzionalnost asimptotskega stožca bomo izpeljali iz končnosti njegove Hausdorffove dimenzije. Pri tem bomo uporabili naslednjo metodo.

Trditev. (KROGLE IN HAUSDORFFOVA DIMENZIJA) Predpostavimo, da lahko metrični prostor X za vsak $\epsilon > 0$ pokrijemo s $k = k(\epsilon)$ kroglami premera kvečjemu ϵ, kjer je $\limsup_{\epsilon\to 0} k \cdot \epsilon^d < \infty$. Tedaj je $\dim_H(X) \le d$.

Dokaz. Naj bo $k(\epsilon) \cdot \epsilon^d < C$ za nek $C > 0$ neodvisen od ϵ. Izberimo $e > d$. Tedaj je

$$\mu_e(X) = \lim_{\epsilon\to 0} \inf_{\{U_i\}_i} \sum_i (\operatorname{diam} U_i)^e \le \lim_{\epsilon\to 0} k(\epsilon) \cdot (\epsilon)^e \le \lim_{\epsilon\to 0} C\epsilon^{e-d} = 0.$$

□

Asimptotski stožec grupe polinomske rasti

Pokažimo najprej, kako polinomska rast grupe vpliva na pokritja podmnožic asimptotskega stožca s kroglami in s tem na Hausdorffovo dimenzijo.

Trditev. Naj bo G grupa polinomske rasti stopnje $d = \deg(G)$. Tedaj obstajata $\epsilon > 0$ in ultrafilter $\mathcal{U}$ na $\mathbb{N}$, za katera za asimptotski stožec K grupe G velja naslednje. Če krogla $B \subseteq K$ polmera 1 vsebuje natanko k točk in če sta vsaki dve točki pri tem oddaljeni za več kot 2ϵ, potem je $k \le (4/\epsilon)^{d+1}$.

Dokaz. Naj bo $\epsilon > 0$ in $\mathcal{U}$ ultrafilter na $\mathbb{N}$, oba zaenkrat še nedoločena. Zaradi homogenosti K lahko predpostavimo, da je $B = B_K(1)$.

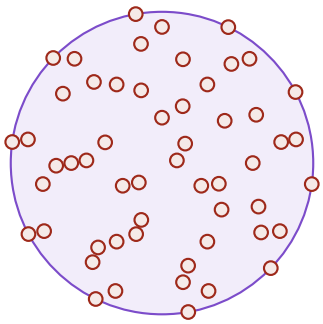
Naj bodo $x_1, \ldots, x_k \in B$ elementi z $d(x_i, x_j) > 2\epsilon$ za $i \ne j$. Naj bo $x_i = [\{g_{i,n}\}_{n\in\mathbb{N}}]$ za neke $g_{i,n} \in G$. Ker je $x_i \in B$, velja $\lim_{\mathcal{U}} d(g_{i,n}, 1)/n \le 1$, zato za vse n iz neke množice $M \in \mathcal{U}$ velja $d(g_{i,n}, 1) \le (1+\epsilon)n$.

Za vsaka $i \ne j$ in naj bo

$$N(i,j,\epsilon) = \{n \in \mathbb{N} \mid d(g_{i,n}, g_{j,n}) > 2\epsilon n\}.$$

[37] Obstoj takega podzaporedja nam zagotovi Fatoujev lema.

[38] Natančneje, ne le za nek r, temveč za vsak r izven množice z Lebesgueovo mero 0.



Slika 5.10: V kroglo $B \subseteq K$ ne moremo vnesti veliko malih disjunktnih kroglic

Ker je $d(x_i, x_j) > 2\epsilon$, velja $N(i,j,\epsilon) \in \mathcal{U}$, zato je tudi

$$N(\epsilon) := \bigcap_{i \neq j} U(i,j,\epsilon) \in \mathcal{U}.$$

Izberimo $r \in \mathbb{N}$ z lastnostjo $2^{-r} < \epsilon \leq 2^{-r+1}$. Naj bo $n \in \mathbb{N}$, $n > r$, z lastnostjo $2^n \in N(\epsilon)$. V *globini* 2^n velja

$$d(g_{i,2^n}, g_{j,2^n}) > 2^{n+1}\epsilon > 2^{n+1-r} = 2 \cdot 2^{n-r},$$

zato so krogle $g_{i,2^n} \cdot B_{G,S}(2^{n-r})$ polmera 2^{n-r} okoli točk $g_{i,2^n}$ disjunktne za $i = 1, \ldots, k$. Od tod sledi

$$\left| \bigcup_{i=1}^{k} g_{i,2^n} \cdot B_{G,S}(2^{n-r}) \right| = k \cdot \beta_{G,S}(2^{n-r}).$$

Hkrati za vsak i velja

$$g_{i,2^n} \cdot B_{G,S}(2^{n-r}) \subseteq B_{G,S}(2^{n-r} + d(g_{i,2^n}, 1)) \subseteq B_{G,S}(2^{n-r} + (1+\epsilon)2^n),$$

slednja krogla pa je vsebovana v $B_{G,S}(2^{n+1})$ za dovolj majhen ϵ.[39] Od tod sledi neenakost

$$k \cdot \beta_{G,S}(2^{n-r}) \leq \beta_{G,S}(2^{n+1})$$

za vse $n > r$, za katere je $2^n \in N(\epsilon)$, pri tem pa je $r = r(\epsilon)$ fiksen.

Za neskončno mnogo naravnih števil a velja

$$\forall b < a\colon \log_2 \beta_{G,S}(2^a) \leq \log_2 \beta_{G,S}(2^{a-b}) + b(d+1).$$

Dokaz: Označimo $L(a) = \log_2 \beta_{G,S}(2^a)$. Ker je $d = \deg(G)$, za vse dovolj velike $a \in \mathbb{N}$ velja $L(a)/\log_2(2^a) < d + \frac{1}{2}$, se pravi $L(a) < a(d+1) - \frac{a}{2}$. V posebnem je $\lim_{a\to\infty}(L(a) - a(d+1)) = -\infty$. Za vsak $k \in \mathbb{Z}$ naj bo a_k najmanjše naravno število, za katerega je $L(a_k) - a_k(d+1) < k$. Tedaj za vse $b < a_k$ velja

$$L(a_k) - a_k(d+1) < k \leq L(a_k - b) - (a_k - b)(d+1),$$

zato je $L(a_k) < L(a_k - b) + b(d+1)$. ✓

[39] Potrebujemo $(1+\epsilon) + 2^{-r} \leq 2$.

Iz pomožne trditve in zadnje neenakosti pred njo izpeljemo[40]

$$k \cdot \beta_{G,S}(2^{n-r}) \leq \beta_{G,S}(2^{n+1}) \leq 2^{(r+1)(d+1)} \cdot \beta_{G,S}(2^{n-r}),$$

kar implicira $k \leq 2^{(r+1)(d+1)} \leq \left(\frac{4}{\epsilon}\right)^{d+1}$. Dokaz je s tem zaključen. □

S pomočjo zadnje trditve lahko omejimo dimenzijo asimptotskega stožca.

Izrek. Naj bo G grupa polinomske rasti in K njen asimptotski stožec glede na ultrafilter iz zadnje trditve. Tedaj ima K končno dimenzijo in je lokalno kompakten.

Dokaz. Končna dimenzija: Dimenzija je lokalna topološka lastnost, zato je dovolj dokazati, da je dimenzija krogle $B = B_K(1)$ končna. V ta namen izberimo maksimalno število točk $x_1, \ldots, x_k \in B$ z lastnostjo $d(x_i, x_j) > 2\epsilon$ za vse $i \neq j$. Iz zadnje trditve sledi $k \leq (4/\epsilon)^{d+1}$. Torej lahko B pokrijemo z $(4/\epsilon)^{d+1}$ kroglami polmera 2ϵ.[41] Iz trditve (KROGLE IN HAUSDORFFOVA DIMENZIJA) sledi $\dim_H(B) \leq d+1$, s tem pa iz izreka (Szpilrajn 1937) sklepamo, da je B končne dimenzije. 𝒻

Lokalna kompaktnost: Dovolj je dokazati, da je vsaka krogla $B \subseteq K$ kompaktna. Naj bo $\{x_n\}_{n\in\mathbb{N}}$ zaporedje v B. Za vsak i pokrijmo B s k_i kroglami polmera kvečjemu 2^{-i}.[42] Izberimo podzaporedje, ki v celoti leži v eni od krogel polmera kvečjemu 1. Po tem izberimo podzaporedje, ki v celoti leži v eni od krogel polmera kvečjemu $\frac{1}{2}$. Po tem izberimo podzaporedje, ki v celoti leži v eni od krogel polmera kvečjemu $\frac{1}{4}$. ... Nazadnje vzemimo podzaporedje, ki sestoji iz prvih členov vseh teh podzaporedij. Po konstrukciji je to Cauchyjevo zaporedje. Iz polnosti K torej sledi, da ima $\{x_n\}_{n\in\mathbb{N}}$ konvergentno podzaporedje. 𝒻 □

Preko stožca do matrik

Asimptotski stožec grupe polinomske rasti ima zdaj veliko dobrih topoloških lastnosti, od koder izpeljemo naslednjo posledico.

Posledica. Bodi G neskončna grupa polinomske rasti. Tedaj obstaja edinka $C \trianglelefteq G$ končnega indeksa v G, da velja vsaj ena od naslednjih trditev.

1. Za nek $k \in \mathbb{N}$ ima C epimorfno sliko D za neko neskončno grupo $D \leq \mathrm{GL}_k(\mathbb{C})$.
2. Obstaja Liejeva grupa Γ s končno mnogo komponentami, tako da za vsak $n \in \mathbb{N}$ obstaja homomorfizem $\varphi_n : C \to \Gamma$ z lastnostjo $|\mathrm{im}\,\varphi_n| \geq n$.

Dokaz. Uporabimo izrek (Montgomery–Zippin 1955) za asimptotski stožec K. Naj bo $\Gamma = \mathrm{Isom}(K)$, opremljena s strukturo Liejeve grupe s

[40] Uporabimo pomožno trditev z $a = n+1$ in $b = r+1$. Pri tem moramo biti nekoliko previdni glede tega, če pomožno trditev sploh lahko uporabimo z $a = n+1$. Naj bo S neskončna množica naravnih števil a, za katere velja pomožna trditev. Naj bo $T = \{2^{a-1} \mid a \in S\}$. Ultrafilter $\mathcal{U}$ izberimo tako, da vsebuje množico T. Za tem izberimo $n \in \mathbb{N}$ z lastnostjo $2^n \in \mathbb{N}_{>2^r} \cap M \cap N(\epsilon) \cap T \in \mathcal{U}$. S tako izbiro n celoten dokaz deluje.

[41] Vsaka točka v B je po maksimalnosti izbire točk $x_1, \ldots, x_k$ namreč največ 2ϵ stran od kakšne od teh točk.

[42] Tako pokritje res obstaja po zadnji trditvi.

končno mnogo komponentami. Torej obstaja abelova edinka $Z \trianglelefteq \Gamma$, da se Γ/Z vloži v $\mathrm{GL}_k(\mathbb{C})$ za nek k. Naj bo $\Phi: G \to \Gamma$ delovanje grupe G na asimptotskem stožcu in naj bo $L = \Phi^{-1}(Z)$. Velja $L \trianglelefteq G$ in $L/\ker\Phi$ je abelova grupa. Obravnavajmo več primerov glede na indeks L oziroma $\ker\Phi$ v G.

- *Če je* $|G:L| = \infty$*:* V tem primeru ima G epimorfno sliko G/L, ki se s Φ vloži v Γ/Z, ta pa se vloži v $\mathrm{GL}_k(\mathbb{C})$. Vzamemo lahko torej $C = G$ (1. točka). ↯

- *Če je* $|G:L| < \infty$ *in* $|G:\ker\Phi| = \infty$*:* V tem primeru ima L epimorfno sliko $L/\ker\Phi$, ki je končno generirana neskončna abelova grupa, zato ima epimorfno sliko $\mathbb{Z}$. Slednja grupa se vloži v $\mathrm{GL}_1(\mathbb{C})$. Vzamemo lahko torej $C = L$ (1. točka). ↯

- *Če je* $|G:\ker\Phi| < \infty$*:* V tem primeru je $\mathrm{im}\,\Phi$ končna. Če je $\ker\Phi$ virtualno abelova grupa, ima torej edinko končnega indeksa z epimorfno sliko $\mathbb{Z}$, ki se vloži v $\mathrm{GL}_1(\mathbb{C})$. Vzamemo lahko torej $C = \ker\Phi$ (1. točka). ↯ Sicer pa po izreku (O DELOVANJU Φ) sledi, da za vsako okolico O identitete id_K najdemo homomorfizem $\varphi_O: \ker\Phi \to \mathrm{Isom}(K)$ z lastnostjo $|\mathrm{im}\,\varphi_O \cap O| > 1$. Po lastnosti (brez malih redov) lahko za vsak $n \in \mathbb{N}$ izberemo okolico O_n, ki ne vsebuje elementov reda kvečjemu n. Slika $\mathrm{im}\,\varphi_{O_n}$ tako vsebuje netrivialen element reda večjega od n, zato je $|\mathrm{im}\,\varphi_{O_n}| > n$. Vzamemo lahko torej $C = \ker\Phi$ (2. točka). ↯ □

Dokaz izreka Gromova

Iz zadnje posledice lahko izluščimo naslednjo lastnost grup polinomske rasti, ki nam bo služila kot odskočna deska za induktiven dokaz izreka Gromova.

Trditev. Bodi G neskončna grupa polinomske rasti. Tedaj obstaja pogrupa $H \leq G$ končnega indeksa v G, ki ima epimorfno sliko $\mathbb{Z}$.

Dokaz. Naj bo C kot v zadnji posledici.

1. Naj bo $\alpha: C \to D$ epimorfizem za neko neskončno grupo $D \leq \mathrm{GL}_k(\mathbb{C})$. Grupe G, C in D so polinomske rasti, zato je D virtualno nilpotentna. Torej obstaja podgrupa $E \leq D$ končnega indeksa v D in zato tudi končnega indeksa v G, za katero je $E/\ker\alpha$ nilpotentna in neskončna podgrupa $\mathrm{GL}_k(\mathbb{C})$. Naj bo $k \in \mathbb{N}$ največje število, za katero je $|E : E^{(k)}| < \infty$. Tedaj je grupa $E^{(k)}$ končnega indeksa v G, njen kvocient $E^{(k)}/E^{(k+1)}$ pa je neskončna končno generirana abelova grupa. Vzamemo lahko torej $H = E^{(k)}$. ↯

2. Naj bo $\varphi_n: C \to \Gamma$ homomorfizem z $|\mathrm{im}\,\varphi_n| > n$ za vsak $n \in \mathbb{N}$. Naj bo $Z \trianglelefteq \Gamma$ abelova edinka, za katero se Γ/Z vloži v $\mathrm{GL}_k(\mathbb{C})$. Naj bo $L_n = \varphi_n^{-1}(Z)$. Torej se grupa C/L_n vloži v Γ/Z, slednja pa se vloži v $\mathrm{GL}_k(\mathbb{C})$.

Izrek (Jordan 1878) zagotovi obstoj podgrupe $K_n \leq C$ omejenega indeksa[43] v C, za katero je $K_n \geq L_n$ in K_n/L_n je abelova grupa. Ker ima grupa C le končno mnogo podgrup danega indeksa, je torej za neskončno mnogo vrednosti n grupa K_n enaka neki fiksni podgrupi $K \leq G$. Za neskončno mnogo naravnih števil n je torej grupa K/L_n abelova.

[43] Indeks $|C : K_n|$ je omejen s funkcijo, odvisno le od k in ne od n.

Če so velikosti grup $|K/L_n|$ neomejene, ima grupa K poljubno velike abelove kvociente. Ker je tudi končno generirana, sledi $|K/K^{(2)}| = \infty$. V tem primeru lahko vzamemo $H = K$. ↙↙

Predpostavimo zdaj, da so velikosti grup $|K/L_n|$ omejene, ko n preteče neko neskončno podmnožico naravnih števil. Ker ima K le končno mnogo podgrup danega indeksa, je za neskončno mnogo vrednosti n grupa L_n enaka neki fiksni podgrupi $L \leq K$. Ker je $|\operatorname{im}\varphi_n| \geq n$ in $|C : L| < \infty$, sledi $\limsup_{n\to\infty} |L/\ker\varphi_n| = \infty$. Grupa $L/\ker\varphi_n$ je abelova, saj se vloži v Z. Torej ima L poljubno veliko abelove kvociente. Ker je tudi končno generirana, sledi $|L : L^{(2)}| = \infty$. Vzamemo lahko torej $H = L$. ↙↙ □

Od tod lahko končno izpeljemo izrek Gromova.

Dokaz izreka Gromova. Naj bo G grupa polinomske rasti stopnje kvečjemu d. Dokazujemo z indukcijo na d. Bazni primer $d = 0$ je mogoče le, ko je grupa G končna in v tem primeru izrek seveda velja. Predpostavimo zdaj, da izrek velja za vse grupe stopnje kvečjemu $d-1$. Po zadnji trditvi obstaja podgrupa $H \leq G$ končnega indeksa v G in $N \trianglelefteq H$, da je $\mathbb{Z} \cong H/N = \langle hN \rangle$ za nek $h \in H$. Po dokazu trditve (PODEKSPONENTNA ⇒ IZVEDENA K.G.) je N končno generirana, hkrati pa je $\deg(N) \leq d-1$. Po indukciji zato obstaja nilpotentna podgrupa $K \leq N$ končnega indeksa v N. Po potrebi K nadomestimo s presekom vseh podgrup v N indeksa $|N : K|$, zato lahko predpostavimo, da je $K \trianglelefteq H$. Naj bo $C = \langle K, h \rangle \leq H$. Velja $H/K = C/K \cdot N/K$, zato je C končnega indeksa v H in s tem tudi v G. Grupa C je razširitev $\mathbb{Z}$ z nilpotentno grupo K, torej je C rešljiva. Ker je C polinomske rasti, od tod sledi, da je C virtualno nilpotentna. Dokaz je s tem zaključen. □

Poglavje 6

Srednja rast

V tem razdelku si bomo ogledali konkreten primer grupe srednje rasti. S tem bomo odgovorili na vprašanje (SREDNJA). Pokazali bomo tudi, kako so te grupe tesno povezane z (ne)obstojem paradoksalnih dekompozicij.

6.1 Grigorčukova grupa

Prvi primer grupe srednje rasti najdemo v (Grigorčuk 1980). Grupa je konstruirana rekurzivno kot grupa nekih posebnih transformacij intervala, mi pa si bomo pogledali njeno ekvivalentno rekurzivno konstrukcijo prek avtomorfizmov drevesa. Videli bomo, da je ravno ta rekurzivnost definicije osrednja pri srednjosti njene rasti.

Avtomorfizmi drevesa

Naj bo $V = \{0,1\}^*$ množica *končnih* nizov s črkama 0 in 1, vključivši prazen niz $\varnothing$. Naj bo $E = \{\{v,w\} \mid v,w \in V,\ w = v0 \text{ ali } w = v1\}$. Na ta način dobimo dvojiško drevo T z vozlišči V in povezavami E. Rečemo, da je drevo T zakoreninjeno v vozlišču $\varnothing$. Za vozlišče $v \in V$ naj bo T_v poddrevo, zakoreninjeno v v. Drevesi T_v in T sta naravno izomorfni.

Opazujmo grupo avtomorfizmov $\mathrm{Aut}(T)$. Vsak avtomorfizem fiksira koren. Naj bosta T_0 in T_1 levo in desno poddrevo drevesa T. Definirajmo avtomorfizem, ki zamenja ti dve poddrevesi:

$$a \in \mathrm{Aut}(T), \quad \varnothing \mapsto \varnothing,\ 0v \mapsto 1v,\ 1v \mapsto 0v \quad (v \in \{0,1\}^*).$$

Jasno je $a^2 = 1$.

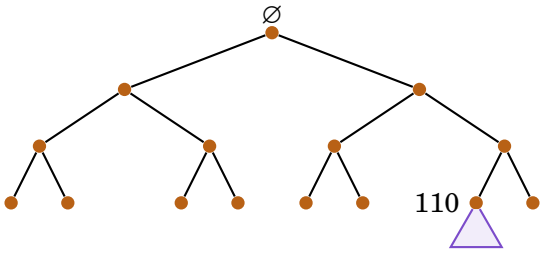
Za poljubno vozlišče v naj $\mathrm{Aut}(T,T_v) \leq \mathrm{Aut}(T)$ sestoji iz tistih avtomorfizmov drevesa T, ki ohranjajo drevo T_v in fiksirajo vozlišča izven T_v. Iz izomorfizma grafov $T \to T_v$ dobimo izomorfizem grup

$$\pi_v : \mathrm{Aut}(T) \to \mathrm{Aut}(T,T_v),$$

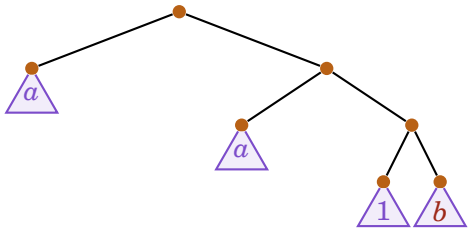
ki avtomorfizem drevesa T prenese na poddrevo T_v. Tako lahko avtomorfizem a prenesemo na poddrevesa in dobimo $a_v = \pi_v(a) \in \mathrm{Aut}(T,T_v)$ za poljubno vozlišče v.

S pomočjo preslikave π_v lahko sestavimo iz dveh avtomorfizmov drevesa enega in dobimo sestavljajoči homomorfizem

$$\sigma : \mathrm{Aut}(T) \times \mathrm{Aut}(T) \to \mathrm{Aut}(T), \quad (\alpha,\beta) \mapsto \pi_0(\alpha) \cdot \pi_1(\beta).$$



Slika 6.1: Drevo T in njegovo poddrevo T_{110}



Slika 6.2: Delovanje elementa $b \in \Gamma$ na drevesu T

S tem lahko rekurzivno definiramo avtomorfizme $b, c, d \in \mathrm{Aut}(T)$:

$$b = \sigma(a, c), \quad c = \sigma(a, d), \quad d = \sigma(1, b).$$

Z drugimi besedami, velja

$$b = \prod_{i=0}^{\infty} (a_{1^{3i}0} \cdot a_{1^{3i+1}0}), \quad c = \prod_{i=0}^{\infty} (a_{1^{3i}0} \cdot a_{1^{3i+2}0}), \quad d = \prod_{i=0}^{\infty} (a_{1^{3i+1}0} \cdot a_{1^{3i+2}0}),$$

kjer smo z 1^i označili niz enic dolžine i. Grigorčukova grupa je grupa $\Gamma = \langle a, b, c, d \rangle \leq \mathrm{Aut}(T)$.

Osnovne lastnosti

V grupi Γ jasno velja $a^2 = 1$. Ker elementi $a_{1^i 0}$ komutirajo za različne vrednosti i, velja tudi $b^2 = c^2 = d^2 = 1$ in $bc = cb = d$, $cd = dc = b$, $bd = db = c$. Torej je $\langle b, c, d \rangle \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Vsak element grupe Γ lahko zapišemo kot besedo s črkami a, b, c, d, pri čemer lahko predpostavimo, da ni zaporednih ponovitev nobene črke in da ni zaporednih ponovitev črk iz množice $\{b, c, d\}$. Tako se v zapisu vsakega elementa grupe Γ izmenjuje črka a in črka iz $\{b, c, d\}$. Taki besedi proste grupe $F(\{a, b, c, d\})$ pravimo alternirajoča beseda.

Zgled. Velja $a^3 b^{-1} c a^2 = abc = ad$.

Najkrajše besede, s katerimi lahko zapišemo elemente v grupi Γ, so alternirajoče.

Lema. Naj bo $g \in \Gamma$, zapisan z besedo $w \in F(\{a, b, c, d\})$ dolžine $\ell(g)$. Potem je w alternirajoča beseda.

Dokaz. Predpostavimo, da $w = x_1 x_2 \ldots x_k$ ni alternirajoča. To je možno le v dveh primerih.

- *Če za nek i velja $x_i = x_{i+1}$:* V tem primeru je $x_i x_{i+1} = x_i^2 = 1$. Beseda $w' = x_1 \cdots x_{i-1} x_{i+2} \cdots x_k$ zato predstavlja element g in je krajše dolžine kot $\ell(g)$. Protislovje.

• *Če za nek i velja $x_i, x_{i+1} \in \{b, c, d\}$:* Ker velja $bc = d, bd = c, cd = b$, je v tem primeru $y := x_i x_{i+1} \in \{b, c, d\}$. Beseda $w' = x_1 \cdots x_{i-1} y x_{i+2} \cdots x_k$ zato predstavlja element g in je krajše dolžine kot $\ell(g)$. Protislovje. □

Grupa Γ inducirano deluje na množici $\{T_0, T_1\}$.[1] Torej dobimo homomorfizem

$$\Gamma \to \mathrm{Sym}(\{T_0, T_1\}).$$

Jedro tega delovanja označimo s H. Grupa H sestoji iz besed, v katerih se element a pojavi sodokrat. Velja torej

$$H = \langle b, c, d, aba, aca, ada \rangle \leq \Gamma \quad \text{in} \quad |\Gamma : H| = 2.$$

Elementi grupe H delujejo na vsakem od poddreves T_0 in T_1. Za element $x \in H$ označimo z x_0 delovanje x na T_0 in z x_1 delovanje x na T_1. Po identifikaciji T_0 in T_1 z drevesom T lahko vidimo x_0, x_1 kot avtomorfizma drevesa T.

Zgled. Za element $b \in H$ je $b_0 = a$ in $b_1 = c$.

Na ta način dobimo razstavljajoči homomorfizem[2]

$$\rho : H \to \mathrm{Aut}(T) \times \mathrm{Aut}(T), \quad x \mapsto (x_0, x_1).$$

Generatorji grupe H se pri tem preslikajo na naslednji način:

$b \mapsto (a, c)$, $c \mapsto (a, d)$, $d \mapsto (1, b)$, $aba \mapsto (c, a)$, $aca \mapsto (d, a)$, $ada \mapsto (b, 1)$.[3]

Od tod sledi, da je $\mathrm{im}\,\rho \leq \Gamma \times \Gamma$. Še več, ker je vsak element grupe H enolično določen s tem, kako deluje na obeh polovicah drevesa T, je preslikava ρ injektivna. S tem smo dobili vložitev grupe H v $\Gamma \times \Gamma$. Ta vložitev ima še dodatno lastnost, da sta preslikavi $\pi_i \circ \rho$ surjekciji za $i = 1, 2$, kjer smo s $\pi_i : \Gamma \times \Gamma \to \Gamma$ označili projekcijo na i-to komponento. Nazadnje ima torej grupa Γ podgrupo indeksa 2, ki ima epimorfno sliko Γ. Zaradi tega je Γ nujno *neskončna* grupa.

Samopodobnost

Kadar imata grupi X in Y izomorfni podgrupi $Z \cong W$, $Z \leq X$, $|X : Z| < \infty$, $W \leq Y$, $|Y : W| < \infty$, potem rečemo, da sta grupi X in Y primerljivi.[4]

Trditev. Grupi Γ in $\Gamma \times \Gamma$ sta primerljivi.

Dokaz. Opazujmo vložitev $\rho : H \to \Gamma \times \Gamma$. Za vsak $g \in \Gamma$ obstaja $x \in H$, da je $x_0 = g$, se pravi $\rho(x) = (g, x_1)$. Hkrati je $\rho(ada) = (b, 1)$, kar po konjugiranju z x postane $\rho((ada)^x) = (b, 1)^{\rho(x)} = (b^g, 1)$. Naj bo $B = \langle\langle b \rangle\rangle \leq G$. Torej slika $\mathrm{im}\,\rho$ gotovo vsebuje grupo $B \times 1 \leq \Gamma \times \Gamma$. Podobno dobimo $\mathrm{im}\,\rho \geq 1 \times B$ in s tem $\mathrm{im}\,\rho \geq B \times B$.

Velja $\langle a, d \rangle \cong D_8$ in $|\Gamma : B| \leq 8$.

[1] Če je $x \in T_0$, potem je $a.x \in T_1$, $b.x \in T_0$, $c.x \in T_0$, $d.x \in T_0$. Podobno velja za $x \in T_1$.
[2] Ta homomorfizem je v bistvu inverz homomorfizma σ.
[3] Ne spreglejmo, da je element d rahlo poseben. To bomo kasneje dobro izkoristili.
[4] Angleško *commensurable*.

Dokaz: Velja $a^2 = d^2 = 1$. Ker je $(ad)^2 = ada \cdot d \in H$, je $\rho((ad)^2) = (b,b)$, ki je reda 2. Ker je ρ vložitev, je zato ad reda 4. Tako po univerzalni lastnosti dobimo surjektiven homomorfizem $\langle s,t \mid s^4, t^2, tst = s^{-1}\rangle \to \langle a,d\rangle$, $s \mapsto ad$, $t \mapsto a$. Ker je $\langle a,d\rangle > \langle ad\rangle \cong \mathbb{Z}/4\mathbb{Z}$, je zadnji homomorfizem nujno izomorfizem. ✓✓

Ker je $\Gamma = \langle a,b,c\rangle$, je grupa Γ/B generirana z odsekoma elementov a in d. Ker je $\langle a,d\rangle \cong D_8$, je res $|\Gamma : B| \leq 8$. ✓✓

Iz pomožne trditve sledi $|\Gamma \times \Gamma : \operatorname{im}\rho| \leq 64$. Tako ima grupa Γ podgrupo končnega indeksa H, ki je izomorfna podgrupi končnega indeksa $\operatorname{im}\rho$ grupe $\Gamma \times \Gamma$. □

Grupa Γ je torej *samopodobna*, kot neke vrste fraktal. Če se ji malce ($|\Gamma : H| < \infty$) približamo, vidimo objekt (H), ki skoraj ($|\Gamma \times \Gamma : \operatorname{im}\rho| < \infty$) izgleda kot dve kopiji ($\Gamma \times \Gamma$) začetnega objekta. Samopodobne grupe nikdar niso polinomske rasti.

Posledica. Γ *ni* polinomske rasti.

Dokaz. Predpostavimo, da je Γ polinomske rasti. Potem je tudi $\Gamma \times \Gamma$ polinomske rasti. Iz zadnje trditve zdaj sledi $\deg(\Gamma) = \deg(\Gamma \times \Gamma)$. Toda $\deg(\Gamma \times \Gamma) = 2 \cdot \deg(\Gamma)$ (→ vaje). Od tod sledi $\deg(\Gamma) = 0$, kar je mogoče le, če je Γ končna. Protislovje. □

Rast

Za analizo rasti grupe $\Gamma = \langle a,b,c,d\rangle$ bomo uporabili preslikavo ρ, ki skrajšuje dolžine elementov.

Lema. Bodi $x \in H$ in $\rho(x) = (x_0, x_1)$. Velja $\ell(x_0), \ell(x_1) \leq \frac{1}{2}(\ell(x) + 1)$.

Dokaz. Zapišimo x kot najkrajši možen alternirajoč produkt elementov u in ava za $u,v \in \{b,c,d\}$. Naj bo število uporabljenih faktorjev enako $2k + r$ za $r \in \{0,1\}$. Torej je x produkt k parov oblike $u \cdot ava$ ali $ava \cdot u$ z morebitnim dodatnim faktorjem na koncu. Vsak tak par je dolžine kvečjemu 4, s preslikavo ρ pa se preslika v dva elementa dolžine kvečjemu 2. Torej v primeru $r = 0$ velja $\ell(x) = 4k$ in $\ell(x_0), \ell(x_1) \leq 2k$, v primeru $r = 1$ pa velja $\ell(x_0), \ell(x_1) \leq 2k + 1$. □

Skupna dolžina x_0 in x_1 je torej $\ell(x_0) + \ell(x_1) \leq \ell(x) + 1$. Če ima x veliko pojavitev črke d, potem je dolžina x_0 oziroma x_1 še krajša, ker je $\rho(d) = (1,b)$ in $\rho(ada) = (b,1)$. Če je v x malo pojavitev črke d, pa morda lahko uporabimo ρ na komponentah x_0, x_1 in pretvorimo pojavitve c v d s prvo uporabo ρ, z drugo pa potem d v 1. Če je malo pojavitev c in d, morda lahko uporabimo ρ trikrat in pretvorimo pojavitve b v c, c v d in nazadnje d v 1 ter s tem še bolj skrajšamo dolžino.

Naj bo $K = \rho^{-1}(H \times H)$. Velja $|H : K| = |\rho(H) : \rho(H) \cap (H \times H)| \leq |\Gamma \times \Gamma : H \times H| = 4$, zato je $|\Gamma : K| \leq 8$. Naj bo še $L = \rho^{-1}(K \times K)$. Kot prej velja $|\Gamma : L| \leq 128$. Za $x \in L$ je $x_0, x_1 \in K$, zato je $x_{00}, x_{01}, x_{10}, x_{11} \in H$ in nazadnje dobimo elemente $x_{000}, x_{001}, \ldots, x_{111} \in \Gamma$. Trdimo, da je skupna dolžina po trikratni uporabi ρ bistveno krajša od originalne dolžine.

Lema. (O KRAJŠANJU DOLŽIN) Bodi $x \in L$. Velja

$$\ell(x_{000}) + \ell(x_{001}) + \cdots + \ell(x_{111}) \leq \frac{5}{6}\ell(x) + 8.$$

Dokaz. Vemo že, da velja $\ell(x_0) + \ell(x_1) \leq \ell(x) + 1$. Naj bo $\ell_b(x)$ število pojavitev črke b v besedi x, zapisani alternirajoče z dolžino $\ell(x)$. Analogno definiramo $\ell_c(x), \ell_d(x)$.

- Vsaka pojavitev črke d ali ada v besedi x postane 1 v natanko enem od x_0, x_1. Od tod sklepamo

  $$\ell(x_0) + \ell(x_1) \leq \ell(x) + 1 - \ell_d(x)^{5}$$

  in zatorej

  $$\begin{aligned}\ell(x_{000}) + \cdots + \ell(x_{111}) &\leq (\ell(x_{00}) + 1) + \cdots + (\ell(x_{11}) + 1) \\ &\leq (\ell(x_0) + 1) + (\ell(x_1) + 1) + 4 \\ &\leq \ell(x) + 7 - \ell_d(x).\end{aligned}$$

- Vsaka pojavitev c ali aca v besedi x postane d v natanko enem od x_0, x_1.[6] Od tod sklepamo

  $$\begin{aligned}\ell(x_{00}) + \cdots + \ell(x_{11}) &\leq \ell(x_0) + 1 + \ell(x_1) + 1 - \ell_c(x) \\ &\leq \ell(x) + 3 - \ell_c(x)\end{aligned}$$

  in zatorej

  $$\begin{aligned}\ell(x_{000}) + \cdots + \ell(x_{111}) &\leq (\ell(x_{00}) + 1) + \cdots + (\ell(x_{11}) + 1) \\ &\leq \ell(x) + 7 - \ell_c(x).\end{aligned}$$

- Vsaka pojavitev b ali aba v besedi x postane c v natanko enem od x_0, x_1. Od tod sklepamo

  $$\begin{aligned}\ell(x_{000}) + \cdots + \ell(x_{111}) &\leq (\ell(x_{00}) + 1) + \cdots + (\ell(x_{11}) + 1) - \ell_b(x) \\ &\leq \ell(x) + 7 - \ell_b(x).\end{aligned}$$

Velja $\ell_b(x) + \ell_c(x) + \ell_d(x) \geq \frac{1}{2}(\ell(x) - 1)$, zato je $\ell_u(x) \geq \frac{1}{6}\ell(x) - 1$ za nek $u \in \{b, c, d\}$. Iz zgornjih neenakosti zato v vsaki od treh možnosti za u sledi

$$\ell(x_{000}) + \cdots + \ell(x_{111}) \leq \ell(x) + 7 - \ell_u(x) \leq \frac{5}{6}\ell(x) + 8.$$

□

S pomočjo krajšanja dolžin lahko nazadnje dokažemo, da Γ ni eksponentne rasti. Vemo tudi že, da Γ ni polinomske rasti, torej s tem odgovorimo na vprašanje (SREDNJA).

Izrek. Γ je srednje rasti.

[5] Na primer, velja $\rho(aba \cdot d \cdot aca) = (c,a)(1,b)(d,a) = (cd, aba) = (b, aba)$.

[6] Pri tem se lahko zgodi, da po eni uporabi ρ dobimo x_0, x_1, ki se še poenostavita, kot v primeru $\rho(aba \cdot d \cdot aca)$.

Dokaz. Naj bo $\omega = \omega_{\{a,b,c,d\}}(\Gamma)$. Dokazati želimo, da je $\omega = 1$.

Najprej prevedimo problem na grupo L. Naj bo R množica predstavnikov odsekov L v Γ. Torej je $\Gamma = L \cdot R$. Naj bo $M = \max\{\ell(r) \mid r \in R\}$. Izberimo poljuben $x \in B_\Gamma(n)$. Zapišemo ga lahko kot $x = yz$ za neka $y \in L, z \in R$. Pri tem velja $\ell(y) \leq \ell(x) + \ell(z) \leq n + M$. Torej je

$$\beta_\Gamma(n) \leq |\Gamma : L| \cdot |\{y \in L \mid \ell(y) \leq n + M\}| \leq 128 \cdot |L \cap B_\Gamma(n + M)|.$$

Oceniti moramo torej še $|L \cap B_\Gamma(n + M)|$. V ta namen izberimo poljuben $x \in L \cap B_\Gamma(m)$ za nek $m \in \mathbb{N}$. Naj bo $m_{ijk} = \ell(x_{ijk})$ za $i, j, k \in \{0, 1\}$. Število možnosti za 8-terico elementov $(x_{000}, \ldots, x_{111})$ je enako kvečjemu $\beta_\Gamma(m_{000}) \cdots \beta_\Gamma(m_{111})$. Po definiciji ω za vsak $\epsilon > 0$ velja $\beta_\Gamma(n) \leq A \cdot (\omega + \epsilon)^n$ za vsak n in neko konstanto A. Torej je število možnosti za $(x_{000}, \ldots, x_{111})$ in s tem za $x \in L \cap B_\Gamma(m)$ kvečjemu

$$A^8 \cdot (\omega + \epsilon)^{m_{000} + \cdots + m_{111}} \leq A^8 \cdot (\omega + \epsilon)^{\frac{5}{6}m + 8} \leq C \cdot (\omega + \epsilon)^{\frac{5}{6}m}$$

za neko konstanto C, kjer smo v prvi neenakosti uporabili lemo (O KRAJŠANJU DOLŽIN).

Za vsak $n \in \mathbb{N}$ nazadnje torej velja

$$\beta_\Gamma(n) \leq 128 \cdot C \cdot (\omega + \epsilon)^{\frac{5}{6}(n+M)}.$$

Hkrati po definiciji ω velja $\beta_\Gamma(n) \geq C' \cdot (\omega - \epsilon)^n$ za neko konstanto C'. Uporabimo n-ti koren, izlimitiramo $n \to \infty$ in dobimo

$$\omega - \epsilon \leq (\omega + \epsilon)^{\frac{5}{6}}.$$

Ker je bil ϵ poljuben, sledi $\omega = \omega^{\frac{5}{6}}$, zato je $\omega = 1$. □

Rastna funkcija Γ ni torej niti polinomska niti eksponentna. Ali je ekvivalentna kateri znani elementarni funkciji?

Izrek. Obstajata števili $0 < p, q < 1$, da je $e^{n^p} \leq \beta_\Gamma \leq e^{n^q}$.

Dokaz. Zgornja meja: Dokaz je v tem primeru bolj natančna različica dokaza zadnjega izreka. Iz leme (O KRAJŠANJU DOLŽIN) sledi, da za nek x_{ijk} velja $\ell(x_{ijk}) \leq \frac{5}{48}\ell(x) + 1$. Za element x_{ijk} imamo torej največ $\beta_\Gamma(\frac{5}{48}\ell(x) + 1)$ možnosti. Za vse druge elemente množice $\{x_{000}, \ldots, x_{111}\} \setminus \{x_{ijk}\}$ pa imamo največ $\beta_\Gamma(\frac{1}{8}\ell(x) + 1)$ možnosti.[7] Po submultiplikativnosti rastne funkcije velja

$$\beta_\Gamma\left(\frac{1}{8}\ell(x) + 1\right) \leq \beta_\Gamma\left(\frac{1}{48}\ell(x) + 1\right)^6.$$

Vseh možnosti za 8-terico $(x_{000}, \ldots, x_{111})$ je torej kvečjemu

$$8^8 \cdot \beta_\Gamma\left(\frac{1}{48}\ell(x) + 1\right)^{6 \cdot 7 + 5}.$$

Kot v dokazu zadnjega izreka od tod sledi

$$\beta_\Gamma(n) \leq 128 \cdot |L \cap B_\Gamma(n + M)| \leq C \cdot \beta_\Gamma\left(\frac{1}{48}n + C\right)^{47}$$

[7] Za $x \in L$ namreč velja $\ell(x_{000}), \ldots, \ell(x_{111}) \leq \frac{1}{8}\ell(x) + 1$, saj za vsak $h \in H$ po prvi lemi v tem razdelku velja $\ell(h_0), \ell(h_1) \leq \frac{1}{2}(\ell(h) + 1)$.

[8] Izbrati moramo element x_{ijk}, za katerega velja strožja neenakost glede dolžine. Za to imamo na voljo 8 možnosti.

za neko konstanto C. To neenakost zdaj iteriramo. V naslednjem koraku dobimo

$$\begin{aligned}\beta_\Gamma(n) &\le C\cdot\left(C\cdot\beta_\Gamma\left(\frac{1}{48}\left(\frac{1}{48}n+C\right)+C\right)^{47}\right)^{47}\\ &= C^{1+47}\cdot\beta_\Gamma\left(\frac{1}{48^2}n+C\left(1+\frac{1}{48}\right)\right)^{47^2},\end{aligned}$$

po t korakih pa dobimo neenakost

$$\beta_\Gamma(n)\le C^{1+47+47^2+\cdots+47^{t-1}}\cdot\beta_\Gamma\left(\frac{1}{48^t}n+C\left(1+\frac{1}{48}+\frac{1}{48^2}+\cdots+\frac{1}{48^{t-1}}\right)\right)^{47^t}.$$

Izberimo $t=\lceil\log_{48}n\rceil$. Tedaj je $n/48^t\le 1$, zato iz zadnje neenakosti dobimo

$$\beta_\Gamma(n)\le C^{47^t}\cdot\beta_\Gamma(D)^{47^t}=E^{47^t}$$

za neki konstanti D,E. Po izbiri t od tod nazadnje sledi

$$\beta_\Gamma(n)\le E^{47^{\log_{48}n+1}}=e^{47\cdot\log E\cdot 47^{\frac{\log n}{\log 48}}}\sim e^{n^{\log_{48}47}},$$

torej v izreku lahko vzamemo $q=\log_{48}47<1$. ✓✓

Spodnja meja: Dokaz je v tem primeru kombinacija samopodobnosti grupe Γ in zgornjega iterativnega argumenta. Funkcija β_Γ je ekvivalentna funkciji $\beta_{\Gamma\times\Gamma}$. Hkrati za $S=\{a,b,c,d\}$ velja $\beta_{\Gamma\times\Gamma,S\times 1\cup 1\times S\cup S\times S}=\beta_\Gamma^2$. Torej obstaja konstanta $C>1$, da je

$$\beta_\Gamma(n)^2\le C\cdot\beta_\Gamma(Cn).$$

To neenakost zdaj iteriramo. V naslednjem koraku dobimo

$$\beta_\Gamma(n)\ge\frac{1}{C}\beta_\Gamma\left(\frac{n}{C}\right)^2,$$

po t korakih pa dobimo neenakost

$$\beta_\Gamma(n)\ge\frac{1}{C^{1+2+4+\cdots+2^{t-1}}}\cdot\beta_\Gamma\left(\frac{n}{C^t}\right)^{2^t}\ge\left(\beta_\Gamma\left(\frac{n}{C^t}\right)/C\right)^{2^t}.$$

Izberimo $t=\lfloor\log_C\frac{n}{m}\rfloor$ za nek dovolj velik m, za katerega je $\beta_\Gamma(m)>C$. Tedaj je $C^t<\frac{n}{m}$, zato je $\beta_\Gamma(n/C^t)>\beta_\Gamma(m)$. Iz zadnje neenakosti tako dobimo

$$\beta_\Gamma(n)\ge(\beta_\Gamma(m)/C)^{2^t}=D^{2^t}$$

za neko konstanto $D>1$. Po izbiri t od tod nazadnje sledi

$$\beta_\Gamma(n)\ge D^{2^{\log_C\frac{n}{m}-1}}\ge e^{\frac{1}{2}\cdot\log D\cdot 2^{-\log_C m}\cdot n^{\log_C 2}}\sim e^{n^{\log_C 2}},$$

torej v izreku lahko vzamemo $q=\log_C 2$. ✓✓ □

V zvezi s tem omenimo še sodoben rezultat (Erschler–Zheng 2020), v katerem avtorja z opazovanjem *roba*[9] grupe Γ dokažeta, da velja celo

$$\lim_{n\to\infty}\log_n\log\beta_\Gamma(n)=p_0,$$

kjer je $p_0=\frac{\log 2}{\log\lambda_0}\approx 0.77$, kjer je λ_0 pozitivna ničla polinoma X^3-X^2-2X-4.

Odprt problem. Znano je, da Grigorčukova grupa *ni* končno prezentirana. Ali obstaja končno prezentirana grupa srednje rasti?

[9] Poissonov rob grupe G, opremljene z verjetnostno porazdelitvijo μ, je množica vseh omejenih μ-harmoničnih funkcij na G. Znana je povezava med rastjo grupe in asimptotiko repa porazdelitve μ s končno entropijo in netrivialnim Poissonovim robom. Obstoj take porazdelitve μ nam torej pove nekaj o rasti grupe G.

6.2 Amenabilnost

Amenabilnost je grupno-teoretična lastnost, ki ima veliko ekvivalentnih definicij in ki povezuje rešljive grupe, podeksponentno rast in paradoksalne dekompozicije.

Obstoj invariantne mere

Grupa G je amenabilna, če ima netrivialno, končno, končno aditivno in translacijsko invariantno mero. Z drugimi besedami, obstaja funkcija $\mu: \mathcal{P}(G) \to \mathbb{R}_{\geq 0}$ z naslednjimi lastnostmi:

- $\mu(G) > 0$, (netrivialnost)
- $\forall A, B \subseteq G\colon A \cap B = \varnothing \Rightarrow \mu(A \cup B) = \mu(A) + \mu(B)$, (končna aditivnost)
- $\forall A \subset G\ \forall x \in G\colon \mu(A \cdot x) = \mu(A)$. (desna translacijska invarianca)

Kadar taka mera obstaja, jo lahko vselej normaliziramo in zato predpostavimo $\mu(G) = 1$. Iz desno translacijsko invariantne mere μ lahko preprosto dobimo levo translacijsko invariantno mero ν, in sicer $\nu(A) = \mu(A^{-1})$ za $A \subseteq G$. Ali lahko dobimo tudi mero, ki je hkrati levo in desno translacijsko invarianta?

Amenabilne grupe so torej ravno grupe, v katerih lahko na smiseln način izmerimo velikosti vseh podmnožic grupe.

Zgled.

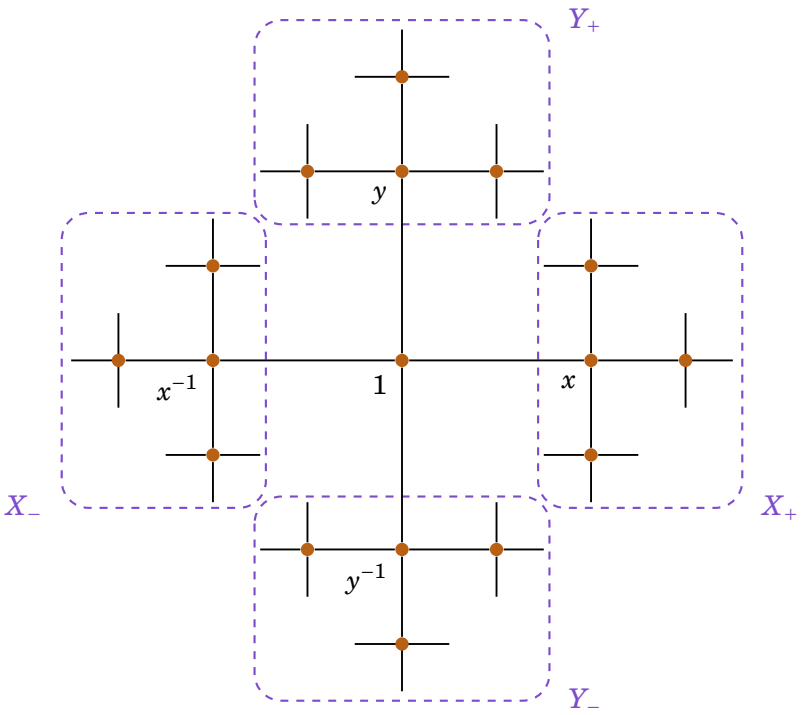
- Naj bo G končna grupa. Za $A \subseteq G$ definirajmo $\mu(A) = |A|/|G|$. To je *edina* mera na G, ki zadošča vsem pogojem za amenabilnost in je hkrati normalizirana.
- Naj bo $G = \mathbb{Z}$. Za $A \subseteq \mathbb{Z}$ in $n \in \mathbb{N}$ definirajmo $A_n = A \cap [-n, n] \subseteq \mathbb{Z}$. Izberimo neglavni ultrafilter $\mathcal{U}$ na $\mathbb{N}$. Definirajmo $\mu(A) = \lim_{\mathcal{U}} |A_n|/n$. S tem dobimo mero, ki zadošča vsem pogojem za amenabilnost. Ta mera pa je daleč od enolične, saj temelji na izbiri ultrafiltra $\mathcal{U}$.
- Naj bo $G = F_2$ prosta grupa ranga 2 z generatorjema x, y. Dokažimo, da F_2 *ni* amenabilna. Zavoljo prostislovja predpostavimo, da je μ *levo* translacijsko invariantna normalizirana mera, ki opazi amenabilnost F_2. Velja $\mu(F_2 \setminus \{1\}) = 1$.[10]

  Naj bo $X_+ \subseteq F_2$ množica okrajšanih besed s prvo črko x, in naj bo X_- množica okrajšanih besed s prvo črko x^{-1}. Sorodno definiramo Y_+, Y_-. Velja $x \cdot Y_+, x \cdot Y_-, x \cdot X_+ \subseteq X_+$ in celo

  $$X_+ = \{x\} \oplus x \cdot Y_+ \oplus x \cdot Y_- \oplus x \cdot X_+.$$

  Od tod sledi $\mu(X_+) = \mu(Y_+) + \mu(Y_-) + \mu(X_+)$, zato je $\mu(Y_+) = \mu(Y_-) = 0$. Podobno izpeljemo $\mu(X_+) = \mu(X_-) = 0$. Od tod nazadnje sledi protislovje $\mu(F_2) = 0$.

[10] Če je namreč $\mu(\{1\}) = p > 1$, potem je $\mu(\{g\}) = p$ za vsak $g \in F_2$ po translacijski invarianci, zato je $\mu(F_2) \geq \sum_g \mu(\{g\})$, kjer vsota teče po poljubni končni množici. To je protislovno z omejenostjo $\mu(F_2)$.



Slika 6.3: Razčlenitev netrivialnih besed v F_2

Integral po meri

Na amenabilnih grupah lahko, kot bomo pojasnili, *integriramo* funkcije s pomočjo mere μ.

Naj bo $f\colon G \to \mathbb{R}$ omejena funkcija, se pravi $a \le f(x) < b$ za vsak $x \in G$. Razdelimo interval $[a,b]$ na podintervale z izbiro delilnih točk $a = a_0 < a_1 < \cdots < a_k = b$. Označimo to izbiro delilnih točk z Δ. Naj bo

$$A_i = \{x \in G \mid a_{i-1} \le f(x) < a_i\}.$$

Velja $G = \bigcup_{i=1}^k A_i$.

Funkcijo f lahko *stopničasto aproksimiramo* s funkcijami, ki so konstantne na vsaki od množic A_i razčlenitve $G = \bigcup_{i=1}^k A_i$. Za vsako od takih aproksimacij $g\colon G \to [a,b]$ lahko izračunamo njeno *delno vsoto* $\sum_{i=1}^k \mu(A_i) \cdot g(A_i)$. Za definicijo vrednosti integrala bosta posebej pomembni delni vsoti

$$S_\Delta = \sum_{i=1}^k \mu(A_i) \cdot a_i \quad \text{in} \quad s_\Delta = \sum_{i=1}^k \mu(A_i) \cdot a_{i-1}.$$

Jasno velja $a \le s_\Delta, S_\Delta \le b$ in $S_\Delta - s_\Delta \le \max_i (a_i - a_{i-1})$.

Če je Δ' finejša izbira delilnih točk kot Δ, potem je $S_{\Delta'} \le S_\Delta$ in $s_{\Delta'} \ge s_\Delta$. Ko torej izbiramo vedno bolj fine delitve,[11] vrednosti S_Δ in s_Δ konvergirata k skupni vrednosti $\inf_\Delta S_\Delta = \sup_\Delta s_\Delta$. To vrednost imenujemo integral funkcije f po grupi G, označimo pa kot $\int_G f \, d\mu$ ali včasih tudi kot $\int_G f(x) \, d\mu(x)$.

Zgled. Naj bo G končna grupa, opremljena z mero $\mu(A) = |A|/|G|$ za $A \subseteq G$. Naj bo $f\colon G \to \mathbb{R}$ funkcija. Tedaj je $\int_G f \, d\mu = \sum_{x \in G} f(x) \cdot \mu(x) = \frac{1}{|G|} \sum_{x \in G} f(x)$, to je povprečje f.

[11] Pri tem mislimo, da izbiramo delitve, pri katerih gre $\max_i (a_i - a_{i-1})$ proti 0. Vsaki dve delitvi imata seveda skupno pofinitev.

V posebnem lahko s pomočjo integrala povprečimo desno-invariantno mero, ki opazi amenabilnost grupe, in dobimo obojestransko invarianco.

Trditev. Bodi G amenabilna. Potem ima G mero, ki opazi njeno amenabilnost in je hkrati levo in desno translacijsko invariantna.

Dokaz. Naj bo μ desno translacijsko invariantna mera, ki opazi amenabilnost G. Definirajmo novo mero ν s predpisom $\nu(A) = \int_G \mu(x \cdot A)\, d\mu(x)$. Trdimo, da je ν iskana mera. Preverimo le, da je ν levo in desno translacijsko invariantna. Z uporabo desne invariantnosti mere μ izpeljemo, da za vsak $y \in G$ velja

$$\begin{aligned}
\nu(y \cdot A) &= \int_G \mu(x \cdot y \cdot A)\, d\mu(x) \\
&= \inf_\Delta \sum_i \mu(\{x \in G \mid a_{i-1} \le \mu(x \cdot y \cdot A) < a_i\}) a_i \\
&= \inf_\Delta \sum_i \mu(\{x \in G \mid a_{i-1} \le \mu(x \cdot A) < a_i\} \cdot y^{-1}) a_i \\
&= \inf_\Delta \sum_i \mu(\{x \in G \mid a_{i-1} \le \mu(x \cdot A) < a_i\}) a_i \\
&= \int_G \mu(x \cdot A)\, d\mu(x) = \nu(A)
\end{aligned}$$

in

$$\nu(A \cdot y) = \int_G \mu(x \cdot A \cdot y)\, d\mu(x) = \int_G \mu(x \cdot A)\, d\mu(x) = \nu(A).$$

□

Osnovne lastnosti amenabilnosti

Amenabilnost je zaprta za vse osnovne konstrukcije grup.

Izrek. Podgrupe in kvocienti amenabilnih grup so amenabilni. Razširitev amenabilne grupe z amenabilno je amenabilna. Končne in abelove grupe so amenabilne.

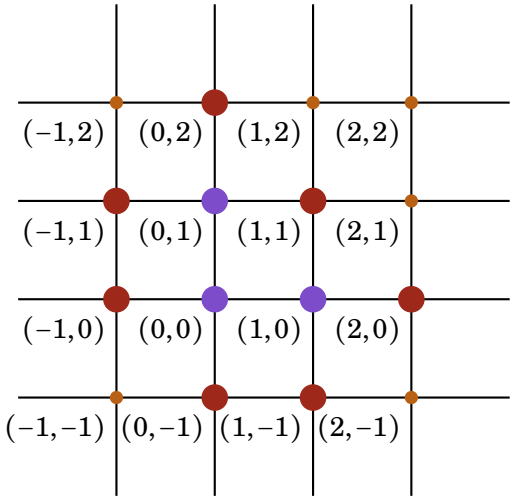
Dokaz. Zaprtost za podgrupe: Naj bo $H \le G$, kjer je G amenabilna. Izberimo neko množico predstavnikov odsekov H v G, recimo ji R. Naj bo $A \subseteq H$. Definirajmo $\mu_H(A) = \mu(R \cdot A)$. Na ta način dobimo želeno mero na H. ✓✓

Zaprtost za kvociente: Naj bo $N \trianglelefteq G$, kjer je G amenabilna. Naj bo $A \subseteq G/N$, torej $A = \{x_\alpha N\}_\alpha$. Definirajmo $\mu_{G/N}(A) = \mu(\bigcup_\alpha x_\alpha N)$. Na ta način dobimo želeno mero na G/N. ✓✓

Zaprtost za razširitve: Naj bo $N \trianglelefteq G$, kjer sta N in G/N amenabilni z merama ν in σ. Naj bo $A \subseteq G$. Definirajmo $f_A : G/N \to \mathbb{R}$, $xN \mapsto \nu(N \cap xA)$. Definirajmo $\mu(A) = \int_{G/N} f_A\, d\sigma$. Na ta način dobimo želeno mero na G. Preverimo le levo translacijsko invariantnost. Za $y \in G$ velja[12]

$$\begin{aligned}
\mu(yA) &= \int_{G/N} f_{yA}(xN)\, d\sigma(xN) \\
&= \int_{G/N} \nu(N \cap xyA)\, d\sigma(xN) \\
&= \int_{G/N} \nu(N \cap xA)\, d\sigma(xN) \\
&= \int_{G/N} f_A(xN)\, d\sigma(xN) = \mu(A).
\end{aligned}$$

[12] Kot v dokazu prejšnje trditve izpeljemo, da je $\int_{G/N} g(xy)\, d\sigma(x) = \int_{G/N} g(x)\, d\sigma(x)$ za vsako funkcijo $g : G/N \to \mathbb{R}$.



Slika 6.4: Rob množice $A = \{(0,0),(0,1),(1,0)\} \subseteq \mathbb{Z}^2$

Končne in abelove grupe: Končne grupe so jasno opremljene z ustrezno mero. Prav tako velja za grupo $\mathbb{Z}$. Od tod in že dokazanih zaprtosti amenabilnosti sledi, da so končno generirane abelove grupe tudi amenabilne. Za neskončno generirane grupe se moramo malo bolj potruditi.

> Naj bo G grupa. Če je vsaka končno generirana podgrupa grupe G amenabilna, potem je tudi G amenabilna.

Dokaz: Opazujmo prostor funkcij $F = [0,1]^{\mathcal{P}(G)}$, opremljen s produktno topologijo. Končno aditivne normalizirane invariantne mere na G tvorijo zaprto podmnožico v F. Naj bo $H \leq G$ končno generirana podgrupa z mero μ_H. Mero razširimo na G z definicijo $\mu(A) = \mu_H(A \cap H)$ za $A \subseteq G$. Ta razširitev je končno aditivna in normalizirana, translacijsko invariantna pa je le glede na elemente v H. Tudi množica vseh takih mer F_H je zaprta v prostoru F in vemo, da je celo neprazna. Denimo, da je presek vseh množic F_H, ko H preteče končno generirane podgrupe grupe G, prazen. Zaradi kompaktnosti F od tod sledi, da obstajajo $H_1,\ldots,H_k$ končno generirane podgrupe grupe G, za katere je $F_{H_1} \cap \cdots \cap F_{H_k} = \emptyset$. Toda množice F_{H_i} vsebujejo F_K, kjer je $K = \langle H_1,\ldots,H_k \rangle$, torej je njihov presek neprazen. Protislovje. Torej res najdemo mero μ v preseku vseh F_H, ki je zato G-invariantna. ✓ □

Iz izreka neposredno sledi, da so rešljive grupe amenabilne. Torej je amenabilnost posplošitev rešljivosti.

Zgled. Heisenbergova grupa in svetilkarjeva grupa sta amenabilni.

Følnerjeva zaporedja

Naj bo $G = \langle S \rangle$. Za množico $A \subseteq G$ definiramo njen rob kot

$$\partial A = \{x \in G \mid \min_{a \in A} d_S(x,a) = 1\}.$$

Zgled. V grupi $\mathbb{Z}^2 = \langle (0,1),(1,0) \rangle$ naj bo $A = \{(0,0),(0,1),(1,0)\}$. Rob te množice je $\partial A = \{(-1,0),(-1,1),(0,2),(1,1),(2,0),(1,-1),(0,-1)\}$.

Rečemo, da grupa G zadošča Følnerjevemu pogoju, če obstaja zaporedje $\{X_n\}_{n=1}^{\infty}$ končnih podmnožic grupe G z lastnostjo $\lim_{n\to\infty} |\partial X_n|/|X_n| = 0$.[13]

Zgled. Opazujmo grupo $\mathbb{Z}^2$. Naj bo $X_n = \{(x,y) \in \mathbb{Z}^2 \mid |x|, |y| \leq n\}$. Velja $|\partial X_n| = 4(2n+1)$ in $|X_n| = (2n+1)^2$, zato je $\lim_{n\to\infty} |\partial X_n|/|X_n| = 0$. Grupa $\mathbb{Z}^2$ torej ima Følnerjevo zaporednje.

Izrek. Končno generirana grupa zadošča Følnerjevemu pogoju, če in samo če je amenabilna.

Dokaz. Dokazali bomo le implikacijo iz leve v desno. Za dokaz obratne implikacije bi potrebovali kar nekaj funkcionalne analize, zato ga izpustimo.

Naj bo X_n Følnerjevo zaporedje v G. Amenabilnost dokažemo kot v zgledu grupe $\mathbb{Z}$. Izberimo neglavni ultrafilter $\mathcal{U}$ na $\mathbb{N}$. Za $A \subseteq G$ naj bo $A_n = A \cap X_n$. Definirajmo $\mu(A) = \lim_{\mathcal{U}} |A_n|/|X_n|$. To je želena mera na G. Preverimo le desno translacijsko invarianco z elementom $s \in S$. Velja $|As \cap X_n| = |A \cap X_n s^{-1}|$ in $A \cap X_n s^{-1} \subseteq A_n \cup \partial X_n$,[14] od koder sledi

$$\frac{|As \cap X_n|}{|X_n|} \leq \frac{|A_n|}{|X_n|} + \frac{|\partial X_n|}{|X_n|}.$$

V limiti je zato $\mu(As) \leq \mu(A) + 0$. Od tod zdaj izpeljemo še drugo neenakost $\mu(A) = \mu(Ass^{-1}) \leq \mu(As)$. S tem je res $\mu(As) = \mu(A)$. □

Zabeležimo pomembno posledico, ki natančneje poveže koncept rasti z amenabilnostjo.

Posledica. Grupe podeksponentne rasti so amenabilne.

Dokaz. Opazujmo množice $X_n = B_{G,S}(n)$. Velja $|X_n| = \beta_{G,S}(n)$ in $|\partial X_n| = \beta_{G,S}(n+1) - \beta_{G,S}(n)$. Ker je G podeksponentne rasti, velja

$$1 = \lim_{n\to\infty} \beta_{G,S}(n)^{1/n} \geq^{15} \liminf_{n\to\infty} \frac{\beta_{G,S}(n+1)}{\beta_{G,S}(n)} \geq 1,$$

zato je $\liminf_{n\to\infty} |\partial X_n|/|X_n| = 1 - 1 = 0$. Torej ima $\{X_n\}_{n\in\mathbb{N}}$ Følnerjevo podzaporedje. □

Zgled. Grigorčukova grupa Γ in svetilkarjeva grupa L sta amenabilni. Iz njiju lahko sestavimo še posebej zanimivo grupo $(\bigoplus_{i\in\Gamma} \mathbb{Z}/2\mathbb{Z}) \rtimes \Gamma$,[16] ki *ni* rešljiva (ima nerešljivi kvocient Γ[17]), je eksponentne rasti (premislimo podobno kot za grupo L) in je amenabilna (razširitev amenabilne z amenabilno).

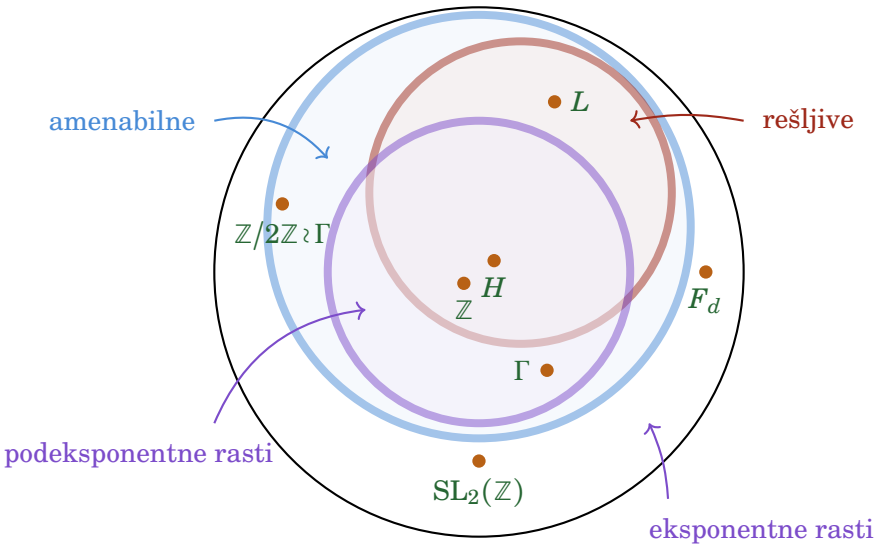
[13] Rob množic X_n je torej v limiti relativno gledano zanemarljiv. Taka grupa je torej *počasne* rasti. *Ortogonalno* definiciji Følnerjevega pogoja so grupe G, za katere velja $\inf_X |\partial X|/|X| > 0$, kjer X preteče vse končne podmnožice grupe G. Take grupe so ekspanzivne in so eksponentne rasti.

[14] Če $a \in A \cap X_n s^{-1}$ ni v ∂X_n, potem je $a \in X_n$, zato je $a \in A_n$.

[15] Konvergenčni radij vrste $\sum_n \beta_{G,S}(n) x^n$ je enak 1.

[16] To grupo označimo krajše kot $\mathbb{Z}/2\mathbb{Z} \wr \Gamma$ in jo imenujemo venčni produkt grup $\mathbb{Z}/2\mathbb{Z}$ in Γ, angleško *wreath product*.

[17] Grigorčukova grupa je končno generirana in srednje rasti, zato po dihotomiji med eksponentno in polinomsko rastjo rešljivih grup ni rešljiva.



Slika 6.5: Diagram amenabilnosti, rešljivosti in podeksponentne rasti

Paradoksalne dekompozicije

Grupa G je paradoksalna, če obstajajo množice $A_1,\dots,A_n,B_1,\dots,B_m \subseteq G$ in elementi $x_1,\dots,x_n,y_1,\dots,y_m \in G$ z lastnostjo

$$G = \bigoplus_{i=1}^{n} A_i \oplus \bigoplus_{j=1}^{m} B_j, \quad G = \bigoplus_{i=1}^{n} x_i A_i = \bigoplus_{j=1}^{m} y_j B_j.$$

Zgled. Trdimo, da je prosta grupa F_2 paradoksalna. Za to le malo popravimo množice, ki so opazile, da F_2 ni amenabilna. Naj bo $X_+ \subseteq F_2$ množica okrajšanih besed s prvo črko x, in naj bo X_- množica okrajšanih besed s prvo črko x^{-1}. Naj bo Y_+ množica okrajšanih besed s prvo črko y skupaj z nepozitivnimi potencami y. Naj bo $Y_- = F_2 \setminus (X_+ \cup X_- \cup Y_+)$. Velja $x^{-1} \cdot X_+ \oplus X_- = F_2$ in $y^{-1} \cdot Y_+ \oplus Y_- = F_2$. Torej je F_2 res paradoksalna.

Paradoksalne grupe torej obstajajo in v njih ni nič protislovnega. Težave se pojavijo, če želimo *meriti* velikosti množic v paradoksalni dekompoziciji.

Izrek. (Tarski 1949) Grupa je paradoksalna, če in samo če *ni* amenabilna.

Dokaz. Dokazali bomo le implikacijo iz leve v desno, ki pojasni, da so paradoksalne grupe res protislovne v primeru, ko lahko merimo velikosti podmnožico z neko mero.

Naj bo G paradoksalna grupa, torej

$$G = \bigoplus_{i=1}^{n} A_i \oplus \bigoplus_{j=1}^{m} B_j, \quad G = \bigoplus_{i=1}^{n} x_i A_i = \bigoplus_{j=1}^{m} y_j B_j.$$

Predpostavimo, da je G amenabilna z normalizirano mero μ. Velja

$$1 = \mu(G) = \sum_{i=1}^{n} \mu(A_i) + \sum_{j=1}^{m} \mu(B_j)$$

in hkrati

$$1 = \mu(G) = \sum_{i=1}^{n} \mu(x_i A_i) = \sum_{i=1}^{n} \mu(A_i), \quad 1 = \mu(G) = \sum_{j=1}^{m} \mu(y_j B_j) = \sum_{j=1}^{m} \mu(B_j),$$

od koder izpeljemo protislovje $1 = 1+1$. □

Delovanja paradoksalnih grup vodijo v paradoksalne dekompozicije množic. Naj grupa G deluje na množici X. Podmnožica $Y \subseteq X$ je *G-paradoksalna*, če obstajajo množice $A_1,\dots,A_n,B_1,\dots,B_m \subseteq Y$ in elementi $x_1,\dots,x_n,y_1,\dots,y_m \in G$ z lastnostjo

$$Y = \bigoplus_{i=1}^{n} A_i \oplus \bigoplus_{j=1}^{m} B_j, \quad Y = \bigoplus_{i=1}^{n} x_i.A_i = \bigoplus_{j=1}^{m} y_j.B_j.$$

Trditev. Naj paradoksalna grupa G deluje *prosto* na množici X. Množica X je tedaj G-paradoksalna.

Dokaz. Naj bo G paradoksalna grupa, torej

$$G = \bigoplus_{i=1}^{n} A_i \oplus \bigoplus_{j=1}^{m} B_j, \quad G = \bigoplus_{i=1}^{n} x_i A_i = \bigoplus_{j=1}^{m} y_j B_j.$$

Izberimo en element iz vsake orbite delovanja G na X, vsi ti predstavniki naj tvorijo množico R. Tedaj zaradi prostosti delovanja velja

$$X = \bigoplus_{i=1}^{n} A_i.R \oplus \bigoplus_{j=1}^{m} B_j.R = \bigoplus_{i=1}^{n} x_i A_i.R = \bigoplus_{j=1}^{m} y_j B_j.R,$$

torej je X res G-paradoksalna. □

Zgled. (Hausdorffov paradoks)[18] Opazujmo delovanje grupe $SO(3)$ na prostoru $\mathbb{R}^3$ z običajnim množenjem matrik z vektorji. Na ta način dobimo inducirano delovanje $SO(3)$ na sferi S^2.

Grupa $SO(3)$ vsebuje prosto grupo F_2: z uporabo izreka (PINGPONG) ni težko dokazati (→ vaje), da je

$$G := \left\langle \begin{pmatrix} \frac{3}{5} & \frac{4}{5} & 0 \\ -\frac{4}{5} & \frac{3}{5} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{3}{5} & -\frac{4}{5} \\ 0 & \frac{4}{5} & \frac{3}{5} \end{pmatrix} \right\rangle \cong F_2.$$

Grupa G je torej paradoksalna. Opazujmo njeno delovanje na S^2. To *ni* prosto delovanje, saj je vsak element $1 \neq g \in SO(3)$ rotacija in ima natanko dve fiksni točki na S^2. Naj bo

$$D = \bigcup_{g \in G \setminus \{1\}} (S^2)^g \subseteq S^2.$$

Ker je G končno generirana grupa, je števna, zato je tudi D števna množica. Grupa G deluje na $S^2 \setminus D$.[19] To delovanje je prosto. Iz zadnje trditve zato sledi, da je $S^2 \setminus D$ paradoksalna glede na delovanje G.

Od tod izpeljemo, da *ne* obstaja števno aditivna funkcija μ na $\mathcal{P}(S^2)$, za katero je $\mu(S^2) = 1$ in $\mu(g \cdot A) = \mu(A)$ za vsaka $A \subseteq S^2, g \in SO(3)$.[20] *Vsem* podmnožicam sfere S^2 torej *ne* moremo na smiseln način prirediti njihove *velikosti* oziroma *mere*. Ta rezultat predstavlja začetno točko *teorije mere*.

[18] Hausdorffov paradoks je soroden bolj znanemu paradoksu (Banach-Tarski 1924).

[19] Če je namreč $x \in S^2 \setminus D$ in $g \in G$ z lastnostjo $g.x \in D$, potem obstaja $h \in G$, da je $h.g.x = g.x$, zato je $x \in (S^2)^{g^{-1}hg}$, torej je $x \in D$. Protislovje.

[20] Za tako funkcijo bi namreč zaradi translacijske invariance nujno veljalo $\mu(d) = 0$ za vsak $d \in D$, torej po števni aditivnosti velja $\mu(D) = 0$ in zato taka funkcija inducira normalizirano funkcijo na $S^2 \setminus D$, ki kot v dokazu izreka (Tarski 1949) vodi v protislovje.

Poglavje 7

Eksponentna rast

V tem poglavju bomo preleteli nekaj znanih rezultatov glede enakomernosti eksponentne rasti. Podali bomo tudi primer grupe eksponentne rasti, ki ni enakomerno eksponentne rasti.

7.1 Enakomerno eksponentna rast

Spomnimo se, za da grupo $G = \langle S \rangle$ eksponentnost rasti merimo z

$$\omega_S(G) = \lim_{n\to\infty} \sqrt[n]{\beta_{G,S}(n)} \quad \text{in} \quad \Omega(G) = \inf_{S\subseteq G,\ \langle S\rangle = G} \omega_S(G).$$

Vemo že, da za prosto grupo F_2 velja $\Omega(F_2) \geq 3$, torej je ta grupa enakomerno eksponentne rasti. V tem razdelku si bomo pogledali, da so v določenih naravnih družinah grup vse grupe eksponentne rasti avtomatično tudi enakomerno eksponentne rasti.

Rešljive grupe

Izrek. (Osin 2003) Rešljiva grupa eksponentne rasti je enakomerno eksponentne rasti.

Dokaz je sicer elementaren, a zahteven. Mi si bomo tu pogledali le en značilen primer izreka,[1] ki je v resnici zelo pomembna sestavina Osinovega dokaza.

Zgled. Opazujmo rešljivo grupo $G = \mathbb{Z}^d \rtimes_\varphi \mathbb{Z}$, kjer je

$$\varphi\colon \mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}^d) = \mathrm{GL}_d(\mathbb{Z}), \quad 1 \mapsto A \in \mathrm{GL}_d(\mathbb{Z}).$$

Predpostavimo, da je $\det(A) = \pm 1$ in da je karakteristični polinom matrike A nerazcepen. Naj bo $\mathrm{Spec}(A)$ množica lastnih vrednosti matrike A.[2] Označimo

$$\Lambda = \max\{|\lambda| \mid \lambda \in \mathrm{Spec}(A)\}.$$

Ker je po predpostavki o determinanti produkt vseh absolutnih vrednosti lastnih vrednosti matrike A enak 1, je $\Lambda \geq 1$. *Predpostavimo*, da je $\Lambda > 1$.[3] Trdimo, da tedaj velja neenakost

$$\Omega(G) \geq 2^{\frac{1}{2\log_2 \Lambda + 4}}.$$

[1] Poseben primer tega primera smo že videli v razdelku o policikličnih grupah.

[2] Vse lastne vrednosti so med sabo različne, ker je karakteristični polinom enostaven.

[3] Če je $\Lambda = 1$, potem ni težko premisliti, da je A nujno končnega reda.

Torej ima grupa G enakomerno eksponentno rast in spodnja meja je odvisna le od Λ.

K dokazu neenakosti pristopimo kot v posebnem primeru $A = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, ki smo ga že obravnavali. Naj bo $G = \langle S \rangle$ za poljubno končno množico S. Izberimo $s \in S$ z lastnostjo $m := \pi(s) > 0$, kjer je $\pi: G \to G/\mathbb{Z}^d \cong \mathbb{Z}$ naravna projekcija. Izberimo še $t \in S$ z lastnostjo $u := [s,t] \in \mathbb{Z}^d \setminus \{0\} \subseteq G$. Velja torej $sus^{-1} = A^m(u) \in \mathbb{Z}^d$.[4]

Naj bo $N = \lfloor \log_\Lambda 2 \rfloor$. Oglejmo si elemente grupe G oblike

$$g_{\epsilon_0,\ldots,\epsilon_n} = \sum_{j=0}^{n} A^{jNm}(u^{\epsilon_j}) \in \mathbb{Z}^d \leq G$$

za $n \geq 1$ in $\epsilon_i \in \{0,1\}$. Za fiksno vrednost n so vsi ti elementi različni med sabo.[5] Torej je število opazovanih elementov enako 2^{n+1}. Hkrati lahko vsak tak element zapišemo v multiplikativni obliki

$$g_{\epsilon_0,\ldots,\epsilon_n} = \prod_{j=0}^{n} s^{jN} u^{\epsilon_j} s^{-jN} = u^{\epsilon_0} s^N u^{\epsilon_1} s^N \cdots s^N u^{\epsilon_n} s^{-nN}.$$

Velja torej

$$\ell_S(g_{\epsilon_0,\ldots,\epsilon_n}) \leq (n+1) \cdot \ell_S(u) + 2nN \leq n(2N+4) + 4.$$

S tem je $\beta_{G,S}(n(2N+4)+4) \geq 2^{n+1}$. Uvedimo $x = n(2N+4)+4$, s tem velja

$$\sqrt[x]{\beta_{G,S}(x)} \geq 2^{\frac{1}{x}\left(\frac{x-4}{2N+4}+1\right)},$$

torej v limiti $n \to \infty$ dobimo

$$\omega_S(G) \geq 2^{\frac{1}{2N+4}} \geq 2^{\frac{1}{2\log_2 \Lambda + 4}}.$$

Linearne grupe

V linearnih grupah imamo na voljo Titsovo alternativo, ki pove, da je linearna grupa G bodisi virtualno rešljiva bodisi vsebuje prosto grupo.

Če linearna grupa vsebuje prosto grupo, je eksponentne rasti. Z natančno analizo dokaza Titsove alternative je Breuillard izpeljal *enakomerno* različico alternative, ki nam pove, da prosto podgrupo vselej najdemo v *omejenem* številu korakov v odvisnosti od dimenzije matrik.

Izrek. (Breuillard 2008) (ENAKOMERNA TITSOVA ALTERNATIVA) Za vsak $d \in \mathbb{N}$ obstaja $N = N(d) \in \mathbb{N}$, da velja naslednje. Za vsako polje K in vsako končno množico $S \subseteq \mathrm{GL}_d(K)$ z lastnostjo $1 \in S = S^{-1}$ velja:

- bodisi je $\langle S \rangle$ virtualno rešljiva
- bodisi množica $S^N = B_{\langle S \rangle, S}(N)$ vsebuje elementa, ki generirata prosto grupo F_2.

[4] V posebnem primeru smo imeli $u = e_1 \in \mathbb{Z}^2$.

[5] Kot v dokazu rasti Osinove grupe definiramo linearno formo $L: \mathbb{C}^d \to \mathbb{C}$ z lastnostjo, da za vsak $v \in \mathbb{C}^2$ velja $LAv = \lambda \cdot Lv$, kjer je $\lambda \in \mathrm{Spec}(A)$ z lastnostjo $|\lambda| = \Lambda$. To formo uporabimo na elementih $g_{\epsilon_0,\ldots,\epsilon_n}$.

Dokaz je precej zahteven in poleg teorije normiranih polj uporabi orodja iz logike, diofantske geometrije in algebraičnih grup. V celoti ga bomo izpustili. Bomo pa pokazali, kako lahko z njegovo uporabo hitro izpeljemo, da so linearne grupe, ki niso virtualno rešljive, nujno *enakomerno* eksponentne rasti, ki je odvisna le od dimenzij matrik.

Posledica. Za vsak $d \in \mathbb{N}$ obstaja $\epsilon = \epsilon(d) > 0$, da velja naslednje. Za vsako polje K in vsako končno generirano linearno grupo $G \leq \mathrm{GL}_d(K)$, ki *ni* virtualno rešljiva, velja $\Omega(G) \geq 1+\epsilon$.

Dokaz. Naj bo $G = \langle S \rangle$. Izrek (ENAKOMERNA TITSOVA ALTERNATIVA) zagotovi $N = N(d)$, za katerega obstajata $a, b \in S^N$, da je $\langle a, b \rangle \cong F_2$. Torej je

$$\omega_S(G) = \lim_{n\to\infty} \sqrt[n]{\beta_{G,S}(n)} = \lim_{n\to\infty} \sqrt[nN]{\beta_{G,S}(nN)}$$

Ker je $\beta_{G,S^N}(n) = \beta_{G,S}(nN)$, je zadnja limita enaka

$$\lim_{n\to\infty} \sqrt[nN]{\beta_{G,S^N}(n)} = \sqrt[N]{\omega_{S^N}(G)} \geq \sqrt[N]{\omega_{\{a,b\}}(G)} \geq \sqrt[N]{3} > 1+\epsilon.$$

□

Iz tega rezultata lahko s *projekcijo* potisnemo eksponentno rast krogel iz neskončnih linearnih grup v končne grupe.

Zgled. Opazujmo grupo $\mathrm{SL}_2(\mathbb{Z})$. Izberimo neko njeno generirajočo množico z dvema elementoma, torej $\langle a, b \rangle = \mathrm{SL}_2(\mathbb{Z})$.[6] Velja $\omega_{\mathrm{SL}_2(\mathbb{Z}),\{a,b\}} \geq 1+\epsilon$, kjer je $\epsilon > 0$ univerzalna konstanta iz zadnje posledice. Za vsak $n \in \mathbb{N}$ velja torej

$$\beta_{\mathrm{SL}_2(\mathbb{Z}),\{a,b\}}(n) \geq c \cdot \left(1 + \frac{\epsilon}{2}\right)^n$$

za neko konstanto c, ki je lahko odvisna od izbire generirajoče množice.

Naj bo $w \in B_{\mathrm{SL}_2(\mathbb{Z}),\{a,b\}}(n)$. Element w reduciramo po modulu p za neko praštevilo p s preslikavo $\pi\colon \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Naj bo A največja absolutna vrednost vnosov matrik $a, b, a^{-1}, b^{-1} \in \mathrm{SL}_2(\mathbb{Z})$. Tedaj je največja absolutna vrednost vnosov matrike w kvečjemu $2^{n-1}A^n$.[7] Če je torej $2^{n-1}A^n < \frac{p}{2}$, potem redukcija π inducira *injektivno* preslikavo

$$B_{\mathrm{SL}_2(\mathbb{Z}),\{a,b\}}(n) \to B_{\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}),\{\pi(a),\pi(b)\}}(n).$$

Za neko konstanto c, odvisno od generirajoče množice, torej za vsak $n \leq c \cdot \log p$ velja

$$\beta_{\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}),\{\pi(a),\pi(b)\}}(n) \geq c \cdot \left(1 + \frac{\epsilon}{2}\right)^n,$$

od koder sledi

$$\beta_{\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}),\{\pi(a),\pi(b)\}}(c \cdot \log p) \geq c \cdot p^{c \log(1+\epsilon/2)} \geq c' \cdot |\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})|^{c'}$$

za neko konstanto c', odvisno od generirajoče množice, a neodvisno od p. V zelo malem številu korakov, primerljivem z $\log|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| \sim \log p$, torej z generatorjema $\pi(a), \pi(b)$ pokrijemo ogromen del grupe $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

[6] Vzamemo lahko na primer $a = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $b = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$.

[7] Iz definicije množenja matrik sledi, da je največja absolutna vrednost vnosov matrike ab kvečjemu $A^2 + A^2 = 2A^2$, matrike aba kvečjemu $2A^2 \cdot A + 2A^2 \cdot A = 4A^3$, ...

Na podlagi teh idej je z orodji iz nekomutativne aditivne kombinatorike (Helfgott 2008) dokazal, da za vsako generirajočo množico H grupe $\mathrm{SL}_2(\mathbb{Z})$ obstaja konstanta $C > 0$, da za vsako praštevilo p velja

$$B_{\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}),\pi(H)}(C \log p) = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}).$$

V le parih korakih, primerljivih z $\log|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})|$, lahko torej pokrijemo *celotno* grupo $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Ta rezultat je bil kasneje ustrezno posplošen na druge generirajoče množice grup $\mathrm{SL}_n(\mathbb{F}_q)$ in je vodil v velik razvoj študija rasti v *končnih* grupah.

Kako je pa z rastjo linearne grupe, ki je virtualno rešljiva? Če je virtualno rešljiva grupa G eksponentne rasti, potem je tudi njena rešljiva podgrupa H eksponentne rasti, zato je po prejšnjem razdelku H enakomerno eksponentne rasti, torej[8] je tudi grupa G enakomerno eksponentne rasti. Ni pa jasno, če lahko tudi za virtualno rešljive linearne grupe eksponentne rasti najdemo spodnjo mejo za njihovo enakomerno rast, ki je odvisna le od dimenzij matrik. Domnevno naj bi to bilo res.

Odprt problem. (Breuillardova domneva) Za vsak $d \in \mathbb{N}$ obstaja $\epsilon = \epsilon(d) > 0$, da velja naslednje. Za vsako končno generirano linearno grupo $G \leq \mathrm{GL}_d(\mathbb{C})$, ki *ni* virtualno *nilpotentna*, velja $\Omega(G) \geq 1 + \epsilon$.

V zvezi s tem omenimo še sodoben rezultat (Breuillard–Varjú 2020), kjer avtorja dokažeta, da je zgornja domneva v primeru $G \leq \mathrm{GL}_2(\bar{\mathbb{Q}})$ *ekvivalentna* znani domnevi (Lehmer 1933) iz teorije števil. Obe domnevi sta še vedno odprti.

7.2 Bartholdijeva grupa

Če izstopimo iz sveta rešljivih in linearnih grup, lahko najdemo grupe neenakomerno eksponentne rasti. Tukaj si bomo ogledali en primer take grupe. Prvi primer je konstuiral (Wilson 2004), mi pa si bomo ogledali poenostavljeno[9] različico tega, ki jo je odkril (Bartholdi 2003).

Konstrukcija

Naj bo $A = \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$, grupa 3×3 matrik nad končnim poljem $\mathbb{Z}/2\mathbb{Z}$. Grupa A naravno deluje na neničelnih vektorjih v prostoru $(\mathbb{Z}/2\mathbb{Z})^3$, ki jih označimo na naslednji način:

$$\mathbf{1} = \begin{pmatrix}1\\0\\0\end{pmatrix}, \quad \mathbf{2} = \begin{pmatrix}0\\1\\0\end{pmatrix}, \quad \mathbf{3} = \begin{pmatrix}1\\1\\0\end{pmatrix}, \quad \mathbf{4} = \begin{pmatrix}0\\0\\1\end{pmatrix}, \quad \mathbf{5} = \begin{pmatrix}1\\0\\1\end{pmatrix}, \quad \mathbf{6} = \begin{pmatrix}0\\1\\1\end{pmatrix}, \quad \mathbf{7} = \begin{pmatrix}1\\1\\1\end{pmatrix}.$$

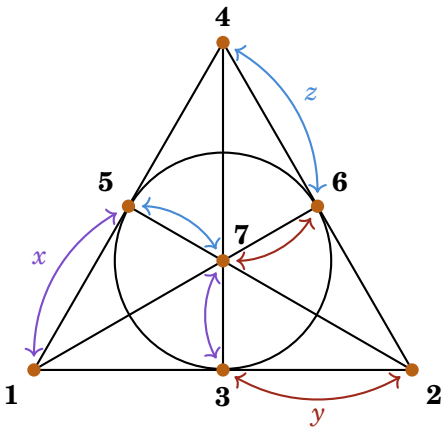
Te vektorje lahko uredimo v Fanovo ravnino, kjer enakoležnost vektorjev na neki premici v tej ravnini pomeni, da so ti vektorji linearno odvisni. Delovanje grupe A ohranja premice v tej ravnini.

Opazujmo naslednje elemente grupe A:

$$x = (\mathbf{1}\ \mathbf{5})(\mathbf{3}\ \mathbf{7}), \quad y = (\mathbf{2}\ \mathbf{3})(\mathbf{6}\ \mathbf{7}), \quad z = (\mathbf{4}\ \mathbf{6})(\mathbf{5}\ \mathbf{7}).$$

[8] Spomnimo se, da za $H \leq G$, $|G : H| < \infty$, velja implikacija $\Omega(H) > 1 \Rightarrow \Omega(G) > 1$.

[9] Kot bomo videli, je poenostavljena različica sicer elementarna, vsekakor pa ni preprosta.



Slika 7.1: Fanova ravnina z delovanji elementov $x, y, z \in A$

Ni težko preveriti, da je $A = \langle x, y, z \rangle$.[10]

Naj bo $P = \{\mathbf{1}, \mathbf{2}, \ldots, \mathbf{7}\} = (\mathbb{Z}/2\mathbb{Z})^3 \setminus \{0\}$. Naj bo P^* množica vseh končnih zaporedij točk iz P. Grupa A deluje *z desne* na P^* na naslednja dva načina:

- *1. način:* Naj bo $a \in A$. Definirajmo $(p_1 p_2 \cdots p_n).a = (p_1.a) p_2 \cdots p_n$.[11]
- *2. način:* Naj bo $a \in A$. Definirajmo $(p_1 p_2 \cdots p_m p_{m+1} \cdots p_n).a$ kot

$$\begin{cases} p_1 \cdots p_m (p_{m+1}.a) p_{m+2} \cdots p_n; & p_1 = \cdots = p_{m-1} = \mathbf{1},\ p_m = \mathbf{2} \\ p_1 \cdots p_n; & \text{sicer.} \end{cases}$$

Naj bo $\bar{A}$ kopija grupe A. Naj A deluje na P^* na 1. način, $\bar{A}$ pa na 2. način. Imamo torej vložitvi $\varphi_1 : A \to \mathrm{Sym}(P^*)$ in $\varphi_2 : \bar{A} \to \mathrm{Sym}(P^*)$. Bartholdijeva grupa je $W = \langle \mathrm{im}\,\varphi_1, \mathrm{im}\,\varphi_2 \rangle \leq \mathrm{Sym}(P^*)$.

Izrek. Grupa W je eksponentne rasti, ni pa enakomerno eksponentne rasti.

Predstavili bomo le glavne poteze dokaza. Kot pri Grigorčukovi grupi dokaz sloni na samopodobnosti grupe W, a na nekoliko drugačen način.

Samopodobnost

Naj bo G poljubna grupa. Opazujmo množico preslikav $P \to G$, ki jo lahko identificiramo z G^7. Ker A deluje na P, dobimo inducirano delovanje A na G^7 z desne. Torej lahko tvorimo semidirektni produkt $G^7 \rtimes A$, ki ga krajše označimo z $G \wr A$. Elemente tega semidirektnega produkta zaradi lažje preglednosti pišemo kot $[g_1, \ldots, g_7]a$ za $g_i \in G, a \in A$.

Kadar grupa G ni čisto poljubna, temveč celo deluje na P^*, dobimo inducirano delovanje grupe $G \wr A$ na P^* na naslednji način:

$$(p_1 p_2 \cdots p_n).[g_1, \ldots, g_7]a = (p_1.a)\left((p_2 p_3 \cdots p_n).g_{p_1}\right).$$

V tem smislu lahko vidimo grupo $G \wr A$ kot podgrupo $\mathrm{Sym}(P^*)$.

[10] Za poljubno matriko $a \in A$ lahko najdemo besedo w v x, y, z, da bo veljalo $w \cdot a.\mathbf{1} = \mathbf{1}$. Po tem lahko najdemo še besedo w', da bo veljalo $w' \cdot w \cdot a.\mathbf{1} = \mathbf{1}$ in $w' \cdot w \cdot a.\mathbf{2} = \mathbf{2}$. Nazadnje lahko najdemo še besedo w'', da $w'' \cdot w' \cdot w \cdot a$ fiksira vse točke. Torej je $a = (w'' \cdot w' \cdot w)^{-1}$.

[11] Element a torej deluje na zaporedju tako, da deluje le na prvi točki.

Vzemimo zdaj $G = W$. Torej je $W \wr A \leq \mathrm{Sym}(P^*)$, hkrati pa je $W \leq \mathrm{Sym}(P^*)$ prek delovanj φ_1, φ_2.

Zgled. Za $a \in A$ velja

$$(p_1 p_2 \cdots p_n).[\bar{a}, a, 1, 1, 1, 1, 1] = \begin{cases} p_1 \cdots p_n; & p_1 \neq \mathbf{1}, \mathbf{2} \\ p_1 (p_2.a) p_3 \cdots p_n; & p_1 = \mathbf{2} \\ p_1 (p_2 \cdots p_n.\bar{a}); & p_1 = \mathbf{1}. \end{cases}$$

Torej element $[\bar{a}, a, 1, 1, 1, 1, 1]$ deluje kot $\bar{a}$ na P^*. Znotraj grupe $\mathrm{Sym}(P^*)$ lahko torej identificiramo $\bar{a} = [\bar{a}, a, 1, 1, 1, 1, 1]$.

Trditev. Identifikaciji W in $W \wr A$ kot podgrupi $\mathrm{Sym}(P^*)$ inducirata izomorfizem $W \cong W \wr A$.

Dokaz. Obravnavajmo W in $W \wr A$ kot podgrupi $\mathrm{Sym}(P^*)$. Iz zadnjega zgleda je razvidno, da velja $\varphi_1(A), \varphi_2(\bar{A}) \leq W \wr A$, zato je $W \leq W \wr A$. Dokazati moramo še obratno vsebovanost.

Izberimo poljubna $a, b \in A$. Tedaj je $[\bar{a}, \bar{b}^y] \in \langle A, \bar{A} \rangle = W$. Velja

$$(p_1 p_2 \cdots p_n).[\bar{a}, \bar{b}^y] = (p_1 \cdots p_n).\bar{a}^{-1} \cdot y^{-1} \bar{b}^{-1} y \cdot \bar{a} \cdot y^{-1} \bar{b} y.$$

Zadnji element je enak

$$\begin{cases} \mathbf{1} \cdots \mathbf{12} (p_{m+1}.a^{-1}) p_{m+2} \cdots p_n . y^{-1} \bar{b}^{-1} y \bar{a} y^{-1} \bar{b} y; & p_1 = \cdots = p_{m-1} = \mathbf{1},\ p_m = \mathbf{2} \\ (p_1 \cdots p_n).y^{-1} \bar{b}^{-1} y \cdot \bar{a} \cdot y^{-1} \bar{b} y; & \text{sicer,} \end{cases}$$

kar se poenostavi do

$$\begin{cases} \mathbf{1} \cdots \mathbf{12} (p_{m+1}.[a, b]) p_{m+2} \cdots p_n; & p_1 = \cdots = p_{m-1} = \mathbf{1},\ p_m = \mathbf{2},\ m > 1 \\ \mathbf{2} p_2 p_3 \cdots p_n; & p_1 = \mathbf{2} \\ p_1 \cdots p_n; & \text{sicer.} \end{cases}$$

Torej je $[[\bar{a}, \bar{b}], 1, 1, 1, 1, 1, 1] = [\bar{a}, \bar{b}^y] \in W$. Ni težko preveriti, da velja $A = [A, A]$, zato od tod izpeljemo $[\bar{A}, 1, 1, 1, 1, 1, 1] \leq W$. Podobno z opazovanjem elementa $[\bar{a}, \bar{b}^x]$ dobimo vsebovanost $[1, A, 1, 1, 1, 1, 1] \leq W$.

Naj bo $t \in A$ in označimo $p = t.\mathbf{1} \in P$. Tedaj je

$$(p p_2 \cdots p_n).t^{-1} [\bar{a}, 1, 1, 1, 1, 1, 1] t = \mathbf{1} (p_2 \cdots p_n.\bar{a}).t = p (p_2 \cdots p_n.\bar{a}),$$

torej je $t^{-1}[\bar{a}, 1, 1, 1, 1, 1, 1]t = [1, \ldots, 1, \bar{a}, 1, \ldots, 1]$, kjer v zadnjem elementu $\bar{a}$ stoji na poziciji p.

S konjugiranjem z ustreznim elementom A torej izpeljemo, da W vsebuje $[1, \ldots, 1, A, 1, \ldots, 1]$ in $[1, \ldots, 1, \bar{A}, 1, \ldots, 1]$, od koder sledi, da W vsebuje celo $[W, W, \ldots, W]$. Ker seveda W vsebuje tudi A, nazadnje izpeljemo želeno vsebovanost $[W, W, \ldots, W] \rtimes A = W \wr A \leq W$. □

Generatorji

Naštejmo par lastnosti glede generatorjev Bartholdijeve grupe.[12] Prva lastnost je ta, da je Bartholdijeva grupa generirana s tremi elementi reda 2, ki jih dobimo iz generatorjev x, y, z grupe A. Naslednja lastnost pa nam pove, da lahko iz generatorjev poljubne grupe G dobimo generatorje grupe $G \wr A$.

[12] Preverjanje teh lastnosti je tehnično zahtevno, a konceptualno podobno premisleku $W \cong W \wr A$, zato dokaze izpustimo.

Trditev.

1. Grupa W je generirana z naslednjimi tremi elementi reda 2:

$$a = [1, \bar{x}, 1, x, 1, 1, 1]x,$$
$$b = [y, 1, 1, \bar{y}, 1, 1, 1]y,$$
$$c = [\bar{z}, z, 1, 1, 1, 1, 1]z.$$

2. Če je grupa G generirana z elementi a, b, c reda 2 in $G = [G, G]$, potem je grupa $G \wr A$ generirana z naslednjimi tremi elementi reda 2:

$$a' = [1, 1, 1, a, 1, 1, 1]x,$$
$$b' = [b, 1, 1, 1, 1, 1, 1]y,$$
$$c' = [1, c, 1, 1, 1, 1, 1]z.$$

Rast

Preverimo najprej, da je Bartholdijeva grupa eksponentne rasti.

Trditev. W je eksponentne rasti.

Ideja dokaza. Trdimo, da grupa W vsebuje prosti monoid na dveh generatorjih. Izberimo $u, v \in A$, $u \neq v$, z lastnostjo $\mathbf{1}.u = \mathbf{1}.v = \mathbf{2}$, $\mathbf{2}.u = \mathbf{2}.v = \mathbf{1}$. Naj bo $a = \bar{u}u$ in $b = \bar{v}v$. Tedaj a in b generirata prosti monoid, saj nobena netrivialna beseda v a, b ne deluje trivialno na P^*. Dokaz tega dejstva izpustimo. □

Zdaj bi radi premislili še, da W ni enakomerno eksponentne rasti. Iz prejšnjega razdelka lahko iterativno dobimo tri generatorje grupe $(((W \wr A) \wr A) \cdots) \wr A$, ki je zaradi samopodobnosti izomorfna grupi W. Pri tem postopku se stopnja rasti glede na dobljene generatorje hitro manjša.

Trditev. Naj grupa G deluje na P. Predpostavimo, da je G generirana z elementi a, b, c reda 2. Naj bo $S = \{a, b, c\}$ in naj bo $S' = \{a', b', c'\}$ iz druge trditve prejšnjega razdelka. Tedaj velja

$$\omega_{S'}(G \wr A) \leq \inf_{\eta \in (0,1)} \max\left\{\omega_S(G)^{1-\eta}, \frac{30^\eta}{\eta^\eta (1-\eta)^{1-\eta}}\right\}.$$

Ideja dokaza. Naj bo w beseda s črkami v S'. Predstavimo jo v obliki $[w_1, \ldots, w_7]\sigma$ za neke besede w_i s črkami v S in $\sigma \in \mathrm{Sym}(P)$. Podobno kot pri Grigorčukovi grupi zdaj analiziramo, kakšne so dolžine besed w_i v odvisnosti od strukture w in kakšna krajšanja se zgodijo v vsaki od besed w_i. □

Nazadnje lahko izpeljemo, da Bartholdijeva grupa *ni* enakomerno eksponentne rasti.

Dokaz $\Omega(W) = 1$**.** Naj bo $S_0 = \{a, b, c\}$ generirajoča množica grupe W iz prve trditve prejšnjega razdelka. Ker so vsi elementi S_0 reda 2, je $\beta_{W,S_0}(n) \leq 3 \cdot 2^{n-1}$, zato je $\omega_{S_0}(W) \leq 2$.

Naj bo $S_{i+1} = S_i'$ za $i \geq 0$, kjer uporabljamo drugo lastnost iz trditve v zadnjem razdelku. Velja

$$\langle S_0 \rangle = W,\ \langle S_1 \rangle = W \wr A \cong W,\ \langle S_2 \rangle = (W \wr A) \wr A \cong W \wr A \cong W, \ldots$$

Po ustrezni identifikaciji v $\mathrm{Sym}(P^*)$ lahko torej množice S_i vidimo kot generirajoče množice grupe W.

Naj bo $\Lambda_0 = 2$. Za $i \geq 0$ naj bo $\eta_i \in (0, \frac{1}{2})$ enolična rešitev enačbe

$$\frac{30^{\eta_i}}{\eta_i^{\eta_i}(1-\eta_i)^{1-\eta_i}} = \Lambda_i^{1-\eta_i}.$$

Za tem definirajmo še $\Lambda_{i+1} = \Lambda_i^{1-\eta_i} > 1$. Ni težko preveriti, da za vsak i velja $0 < \eta_{i+1} < \eta_i$, zato obstaja limita $\eta = \lim_{i\to\infty} \eta_i \geq 0$. Podobno za vsak i velja $1 < \Lambda_{i+1} < \Lambda_i$, zato obstaja limita $\Lambda = \lim_{i\to\infty} \Lambda_i \geq 1$.

Iz definicije η_i in Λ_i sledi enakost $\Lambda^{1-\eta} = \Lambda$, kar implicira $\Lambda = 1$ ali $\eta = 0$. V slednjem primeru sledi $\Lambda = 1$, torej v obeh primerih sklepamo $\Lambda = 1$. Hkrati po zadnji trditvi za vsak i velja neenakost $\omega_{S_i}(W) \leq \Lambda_i$. Od tod sledi $\Omega(W) \leq \lim_{i\to\infty} \omega_{S_i}(W) = 1$. Dokaz je zaključen. □