UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Jaša Knap

KRATKI ZAKONI V GRUPAH

Delo diplomskega seminarja

Mentor: doc. dr. Urban Jezernik

Ljubljana, 2024

Kazalo

Kratki zakoni v grupah

Povzetek

Bistvo diplomske naloge je predstaviti različne konstrukcije kratkih netrvialnih zakonov v grupah. Pri tem obravnavamo naravne družine grup, ki se pri tem pojavijo, kot so na primer nilpotentne, rešljive, enostavne in simetrične. Na koncu predstavimo, kako se iskanja zakonov lotimo z uporabo računalnika.

Short Group Laws

Abstract

The purpose of this thesis is to present various constructions of short group laws. In order to do so, we examine the properties of nilpotent, solvable, simple, and symmetric groups. The thesis is concluded by illustrating how computational methods can be used to discover group laws.

Math. Subj. Class. (2020): 20F10, 20F14, 20D15, 20B30

Ključne besede: zakoni v grupah, proste grupe, nilpotentne grupe, rešljive grupe, enostavne grupe, simetrične grupe, naključni sprehodi po grafih, Cayleyjevi grafi, računalniško iskanje zakonov

Keywords: group laws, free groups, nilpotent groups, solvable groups, simple groups, symmetric groups, random walks on graphs, Cayley graphs, computer-aided

1 Uvod

Začnimo z inuitivno definicijo zakona v grupi, ki jo bomo v nadaljevanju natančneje formulirali s pomočjo prostih grup. Abstraktni produkt elementov $a_1, \ldots, a_k$ ter njihovih inverzov $a_1^{-1}, \ldots, a_k^{-1}$ je *k-črkovni zakon v grupi G*, če ima lastnost, da za vsako zamenjavo $a_1, \ldots, a_k$ s konkretnimi elementi $g_1, \ldots, g_k \in G$ dobimo rezultat $1_G \in G$. Zakonu 1 pravimo *trivialni zakon*, ki v kontekstu raziskovanja zakonov ni posebej zanimiv.

Najosnovnejši primer netrivialnega dvočrkovnega zakona se pojavi pri Abelovih grupah. Grupa G je namreč Abelova natanko tedaj, ko za vsaka elementa $g, h \in G$ velja $gh = hg$, kar je ekvivalentno zahtevi

$$ghg^{-1}h^{-1} = [g, h] = 1_G.$$

Grupa G je torej Abelova natanko tedaj, ko je štiričrkovna beseda $aba^{-1}b^{-1}$ v njej zakon.

Nadvse pomembno je vprašanje, ali vsaka grupa premore netrivialni zakon. Odgovor nanj je v splošnem negativen, kar bomo videli v nadaljevanju kot posledico trditve 5.8. Očitna posledica Lagrangeevega izreka pa je, da vsaka končna grupa G premore netrivialni zakon $a^{|G|}$, saj za vsak element $g \in G$ velja

$$g^{|G|} = 1_G.$$

To dejstvo si natančneje oglejmo na primeru simetrične grupe $\mathrm{Sym}(n)$. Zanjo po Lagrangeevem izreku velja enočrkovni zakon $a^{n!}$, katerega dolžina znaša $n!$, kar je po Stirlingovi formuli približno

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.$$

Asimptotsko gledano je to zelo dolg zakon, veliko krajši je na primer že zakon oblike $a^{\exp(\mathrm{Sym}(n))}$, kjer smo označili $\exp(\mathrm{Sym}(n)) = \mathrm{lcm}(1, \ldots, n)$. Zanj z upoštevanjem leme 2.27 velja dobimo asimptotsko oceno

$$\mathrm{lcm}(1, \ldots, n) \sim \exp(n).$$

Trenutno najboljša ocena za dolžine kratkih zakonov v simetričnih grupah izhaja iz članka [12] in bo predstavljena v razdelku 5.1.

Na tej točki se naravno pojavi nekaj vprašanj: kako dolgi so najkrajši netrivialni zakoni za določeno grupo oziroma družino grup? Ali lahko ocenimo asimtotsko rast dolžine najkrajših netrivialnih zakonov v družinah grup, recimo za družino $\mathrm{Sym}(n)$? Kaj pa za vse grupe moči n ali manj? Katere družine grup se še posebej naravno pojavljajo pri takšnem raziskovanju? Prav ta vprašanja bodo bistvo diplomske naloge, v kateri bom predstavil dosedanje rezultate ter različne pristope, ki so jih ubrali raziskovalci. Na koncu bom predstavil, kako lahko z uporabo računalnika dobimo vpogled v delež zakonov med vsemi besedami.

Zgodovinsko gledano so vprašanja v povezavi z asimptotskimi lastnostmi zakonov razmeroma sodobna. V splošnem pa obravnavanje lastnosti zakonov v nekem smislu sega že do Abela in Galoisa, saj lahko tako Abelove kot rešljive grupe zelo naravno karakteriziramo s pomočjo zakonov. Zakoni so pomembni tudi za obravnavo klasičnih Bursidovih problemov, ki matematikom burijo domišljijo že od začetka 20. stoletja. Ti problemi sprašujejo po končnosti specifičnih kvocientov prostih grup, kar bo nekoliko podrobneje razloženo v razdelku 6.

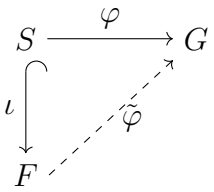
2 Osnovni pojmi za obravnavo zakonov

Za natančno formulacijo in razumevanje zakonov moramo uvesti pojem proste grupe.

2.1 Proste grupe

Naslednjo definicijo proste grupe najdemo v članku [20].

Definicija 2.1. Grupa F je *prosta* nad neprazno množico S, če obstaja preslikava $\iota : S \to F$, da za vsako grupo G in vsako preslikavo $\varphi : S \to G$ obstaja natanko en homomorfizem $\tilde{\varphi} \in \mathrm{Hom}(F, G)$, da velja $\tilde{\varphi} \circ \iota = \varphi$. Z drugimi besedami, spodnji diagram komutira. Tej lastnosti pravimo *univerzalna lastnost prostih grup.*



Opomba 2.2. Preslikava ι v definiciji proste grupe je injektivna. Rečemo ji *standardna inkluzija.*

Dokaz. Dokaz je povzet po odgovoru [3]. Naj bo F prosta grupa nad neprazno množico S. Če je $|S| = 1$, ni kaj dokazovati. Zato predpostavimo, da ima S vsaj dva različna elementa.

Denimo, da ι ni injektivna. Potem obstajata različna elementa $s_1, s_2 \in S$, za katera velja $\iota(s_1) = \iota(s_2)$. Opazujemo preslikavo $\varphi : S \to C_2 = \{1, q\}$ s predpisom $\varphi(s_1) = q$ in $\varphi(s) = 1$ za vse $s \in S \setminus \{s_1\}$. Ker je F prosta, obstaja enolično določen homomorfizem $\tilde{\varphi} : F \to C_2$, da velja $\tilde{\varphi} \circ \iota = \varphi$. Zapišemo

$$\tilde{\varphi}(\iota(s_1)) = \varphi(s_1) = q \neq 1 = \varphi(s_2) = \tilde{\varphi}(\iota(s_2)).$$

Ker je $\tilde{\varphi}$ preslikava, bi moralo veljati $\iota(s_1) \neq \iota(s_2)$, s čimer smo prišli do protislovja. □

V nadaljevanju bomo potrebovali naslednjo preprosto lemo.

Lema 2.3. *Naj bo G končna grupa in F prosta grupa nad k-množico S za $k \geq 1$. Potem velja*

$$|\mathrm{Hom}(F, G)| = |G|^k.$$

Dokaz. Najprej dokažimo $|\mathrm{Hom}(F, G)| \geq |G|^k$. Po definiciji proste grupe nam vsaka preslikava $\varphi : S \to G$ inducira enolično določen homomorfizem $\tilde{\varphi} \in \mathrm{Hom}(F, G)$, da velja $\tilde{\varphi} \circ \iota = \varphi$. To pomeni, da različni preslikavi $\varphi_1, \varphi_2 : S \to G$ inducirata različna homomorfizma $\tilde{\varphi}_1, \tilde{\varphi}_2 \in \mathrm{Hom}(F, G)$, saj bi v nasprotnem primeru imeli

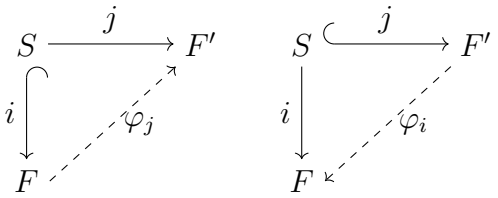
$$\varphi_1 = \tilde{\varphi}_1 \circ \iota = \tilde{\varphi}_2 \circ \iota = \varphi_2.$$

Ker je različnih preslikav $\varphi : S \to G$ natanko $|G|^k$, smo dokazali $|\mathrm{Hom}(F, G)| \geq |G|^k$.

Neenakost $|\mathrm{Hom}(F,G)| \leq |G|^k$ dokažemo z razmislekom, da različna homomorfizma iz $\mathrm{Hom}(F,G)$ lahko induciramo z različnima preslikavama $S \to G$. Naj bo $\psi' \in \mathrm{Hom}(F,G)$. Ker je po opombi 2.2 standardna inkluzija injektivna, vsebuje prosta grupa F vsaj k različnih elementov, ki jih označimo s $s'_1 = \iota(s_1), \ldots, s'_k = \iota(s_k)$. Če definiramo preslikavo $\psi : S \to G$ s predpisom $\psi(s_i) := \psi'(s'_i) = \psi'(\iota(s_i))$, vidimo, da velja $\psi' = \tilde{\psi}$. S tem smo dokazali želeno neenakost, saj različna homomorfzima $\psi'_1, \psi'_2 \in \mathrm{Hom}(F,S)$ zaradi enoličnosti po univerzalni lastnosti ne moreta biti inducirana z isto preslikavo $\psi : S \to G$. □

Trditev 2.4. *Naj bo S neprazna množica. Potem do izomorfizma natančno obstaja največ ena prosta grupa nad množico S.*

Dokaz. Dokaz trditve je vzet iz [20, str. 4]. Naj bosta F in F' prosti grupi nad množico S. Označimo z i in j inkluziji $i : S \to F$ in $j : F'$, ki jima po definiciji 2.1 pripadata. Po univerzalni lastnosti prostih grup lahko inkluziji razširimo do homomorfizmov $\varphi_i : F' \to F$ in $\varphi_j : F \to F'$. Kompozitum $\varphi_i \circ \varphi_j : F \to F$ je na množici S identiteta. Ker sta tako $\varphi_i \circ \varphi_j$ kot id_F razširitvi inkluzije i, mora po enoličnosti razširitev veljati $\varphi_i \circ \varphi_j = \mathrm{id}_F$. Simetrično pokažemo še $\varphi_j \circ \varphi_i = \mathrm{id}_{F'}$, torej sta grupi F in F' izomorfni.



□

Zaradi te trditve je $F(S)$ upravičena oznaka za prosto grupo nad množico S. Še več, grupi $F(S)$ in $F(T)$ sta si izomorfni kot grupi natanko tedaj, ko sta si S in T izomorfni kot množici. Zato bomo v primeru, ko je S končna množica moči k, namesto $F(S)$ pisali F_k. To grupo imenujemo *prosta grupa ranga k*.

Naj bo S poljubna neprazna množica. Definirajmo grupo okrajšanih besed nad množico S kot

$$S^* := \{s_1 s_2 \cdots s_n | n \in \mathbb{N}, \forall i = 1, \ldots, n.\, s_i \in S \cup S^{-1}, \forall i = 1, \ldots n-1.\, s_i \neq s_{i+1}^{-1}\}.$$

Operacija v njej je stikanje besed, ki jim naknadno še okrajšamo sosednje inverze. Ta operacija je dobro definirana, grupa S^* pa prosta nad množico S. Ti dejstvi sta natančno dokazani v viru [13, str. 4, trditev 1.9]. Po trditvi 2.4 sledi $S^* \cong F(S)$, zato si lahko elemente prostih grup predstavljamo kot okrajšane besede. Z upoštevanjem tega dejstva lahko elementom proste grupe $F(S)$ definiramo dolžino.

Definicija 2.5. Naj bo okrajšana beseda $w \in F(S)$ oblike $w = s_1 \cdots s_n$. Potem število $l(w) := n$ imenujemo *dolžina besede w*.

Opomba 2.6. Po definiciji množenja besed v prostih grupah je očitno, da za vsaki besedi w_1, w_2 velja trikotniška neenakost $l(w_1 w_2) \leq l(w_1) + l(w_2)$.

Pri konstrukciji zakonov stalno uporabljamo naslednjo na videz očitno trditev, ki jo vendarle moramo dokazati.

Trditev 2.7. *Proste grupe so* torzijsko proste. *Z drugimi besedami, vsi elementi razen enote so neskončnega reda.*

Dokaz. Dokaz je povzet po odgovoru [2]. Naj bo w netrivialna okrajšana beseda dolžine $l = l(w)$ iz proste grupe $F(S)$. Trdimo, da jo lahko neko celo število $0 \leq r \leq l$ zapišemo v obliki

$$w = s_1 \cdots s_r s_{r+1} \cdots s_{l-r} s_r^{-1} \cdots s_1^{-1} = \beta\alpha\beta^{-1},$$

kjer zahtevamo $s_{r+1} \neq s_{l-r}^{-1}$. Naj bo okrajšana beseda oblike

$$w = a_1 \cdots a_l.$$

Če imamo $a_1 \neq a_l^{-1}$ vzamemo $r = 0$ in zaključimo. Sicer v primeru $a_2 \neq a_{l-2}^{-1}$ vzamemo $r = 1$ in tako dalje. Ker je beseda w nerivialna, velja $l > 0$, zato moramo po končnem številu korakov dobiti ustrezno šteivlo r, saj dosežemo sredino besede w tako z leve kot z desne strani. Če je l sodo število, do tega ne more priti, saj bi dobili besedo oblike $w = \beta\beta^{-1}$, ki ni okrajšana. Če je l liho število pa bi dobili besedo oblike $w = \beta a_{(l+1)/2}\beta^{-1}$, torej lahko vzamemo $r = (l+1)/2$.

Za poljubno naravno število n torej velja

$$w^n = \beta\alpha^n\beta^{-1}.$$

Po konstrukciji besed α in β ne more priti do krajšanja na stičiščih $\beta\alpha$, $\alpha\alpha$ ali $\alpha\beta^{-1}$, zato je w^n okrajšana beseda. S tem smo dokazali, da ima vsak netrivialni element v prosti grupi neskončni red. □

Brez dokaza bomo privzeli Nielsen–Schreierjev izrek, ki je klasični rezultat v teoriji prostih grup. Potrebovali ga bomo za dokaz komutatorske leme, še bolj izrazito pa pri obravnavi zakonov z računalnikom v razdelku 6.

Izrek 2.8 (Nielsen–Schreier)**.** *Vsaka podgrupa proste grupe je prosta.*

Bralec lahko dokaz najde v [13, str. 5–8].

2.2 Definicija in osnovne lastnosti zakonov

Za začetek uvedimo blago zlorabo notacije. Naj bo podana prosta grupa $F_k = \langle a_1, \ldots, a_k \rangle$ in naj bo w beseda v njej. Naj bo G grupa in naj bodo $g_1, \ldots, g_k \in G$. Potem definiramo

$$w(g_1, \ldots, g_k) := \varphi(w),$$

kjer je $\varphi \in \mathrm{Hom}(F_k, G)$ po univerzalni lastnosti induciran s slikami $a_i \mapsto g_i$ za $i = 1, \ldots, k$. To je formalna definicja intuitivne ideje „vstavljanja konkretnih elementov grupe v abstraktne elemente“ iz uvodnega poglavja. Z njeno pomočjo definiramo zakone.

Definicija 2.9. Beseda $w \in F_k$ je *k-črkovni zakon v grupi G*, če za vse k-terice elementov $g_1, \ldots, g_k \in G$ velja $w(g_1, \ldots, g_k) = 1_G$. Za vsako podgrupo $H \leq G$ pravimo, da je $w \in F_k$ *k-črkovni zakon v podgrupi H*, če za vse k-terice elementov $h_1, \ldots, h_k \in H$ velja $w(h_1, \ldots, h_k) = 1_G$.

Ta definicija nam omogoča vpogled v strukturo zakonov. Naj $K(G,k) \subseteq F_k$ *označuje množico k-črkovnih zakonov v grupi G*. Potem v luči prejšnje definicije velja

$$K(G,k) = \bigcap_{\varphi \in \mathrm{Hom}(F_k, G)} \ker(\varphi).$$

Ta množica je končni presek edink v G in posledično tudi sama edinka. Še več, je karakteristična, saj za vsak avtomorfizem $\alpha \in \mathrm{Aut}(F_k)$ velja

$$K(G,k) = \bigcap_{\varphi \in \mathrm{Hom}(F_k, G)} \ker(\varphi) = \bigcap_{\varphi \in \mathrm{Hom}(F_k, G)} \ker(\varphi \circ \alpha).$$

To je preprosta posledica dejstva, da φ preteče grupo $\mathrm{Hom}(F_k, G)$ natanko tedaj, ko jo preteče $\varphi \circ \alpha$.

Lema 2.10. *Naj bo G grupa ter $H_1, \ldots, H_n$ njene podgrupe končnega indeksa, torej $[G : H_i] < \infty$ za $i = 1, \ldots, n$. Potem je tudi $\bigcap_{i=1}^n H_i$ podgrupa končnega indeksa v G in velja*

$$\left[G : \bigcap_{i=1}^n H_i\right] \leq \prod_{i=1}^n [G : H_i].$$

Dokaz. Dovolj je dokazati trditev za $n = 2$, za višje vrednosti sledi z indukcijo. Naj bosta $H_1, H_2 \leq G$ podgrupi končnega indeksa, označimo $S := H_1 \cap H_2$, ki je podgrupa v G. Naj bosta A_1 in A_2 množici odsekov podgrup H_1 in H_2 v G ter naj bo A množica odsekov podgrupe S v G. Definiramo preslikavo $f \colon A \to A_1 \times A_2$ s predpisom $f(gS) = (gH_1, gH_2)$. Desna smer sklepa

$$gS = hS \iff gh^{-1} \in H_1,\ gh^{-1} \in H_2 \iff gH_1 = hH_1,\ gH_2 = hH_2$$

dokaže dobro definiranost preslikave f, leva pa njeno injektivnost, ki nam podaja oceno $|A| \leq |A_1||A_2|$. □

Posledica 2.11. *Naj bo G končna grupa in k naravno število. Potem je grupa zakonov $K(G,k)$ podgrupa končnega indeksa največ $|G|^{|G|^k}$ v F_k.*

Dokaz. Za vsak homomorfizem $\varphi \in \mathrm{Hom}(F_k, G)$ po prvem izreku o izomorfizmu velja

$$|F_k / \ker \varphi| = |\mathrm{im}\, \varphi| \leq |G|,$$

po drugi strani pa po lemi 2.3 velja $|\mathrm{Hom}(F_k, G)| = |G|^k$. Ti dejstvi z uporabo 2.10 povežemo v želeno oceno. □

To dejstvo bo še posebej pomembno pri iskanju zakonov z računalnikom.

Definicija 2.12. Naj bo G grupa in $S \subseteq G$ njena *simetrična* podmnožica. To pomeni, da velja $S = S^{-1} := \{s^{-1} | s \in S\}$. Potem $\mathrm{Cay}(G, S)$ označuje graf z vozlišči $V = G$ in povezavami $E = \{(p, q) | p^{-1}q \in S\}$. Imenujemo ga *Cayleyjev graf grupe G, generiran z množico S*.

Opomba 2.13. Pogoj simetričnosti $S = S^{-1}$ nam pove, da je $\mathrm{Cay}(G, S)$ pravi graf in ne zgolj usmerjeni. Imamo namreč

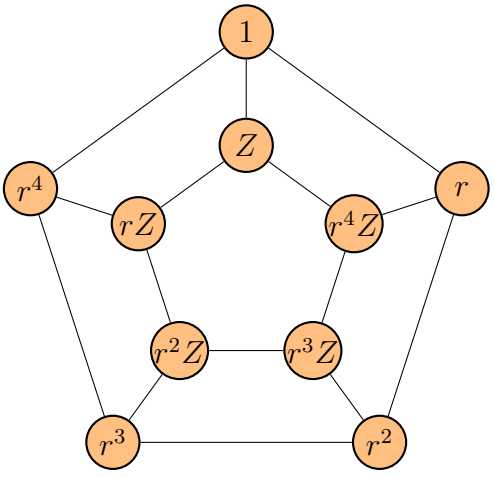
$$(p, q) \in E \iff p^{-1}q \in S \iff q^{-1}p \in S \iff (q, p) \in E.$$

Preden si ogledamo dva primera, dokažimo naslednjo preprosto, a pomembno trditev.

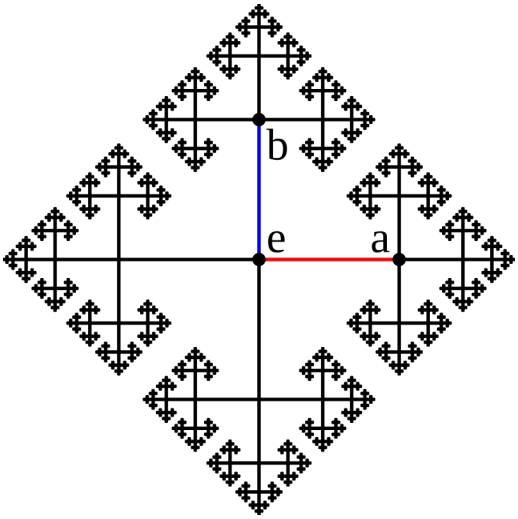
Trditev 2.14. *Naj bo G končna grupa, generirana s k-množico S. Cayleyjev graf $Cay(G, S)$ je k-regularen, povezan graf.*

Dokaz. Naj bo $g \in G$ vozlišče Cayleyjevega grafa $\mathrm{Cay}(G, S)$. Potem je g povezano z enoto 1_G, saj je $\langle S \rangle = G$, torej lahko zapišemo $g = s_1 s_2 \cdots s_n$ za neke elemente $s_i \in S$. Ta produkt določa pot v Cayleyjevem grafu. Ker je vsako vozlišče povezano z enoto 1_G, je graf povezan. Iz $gs_i = gs_j$ sledi $s_i = s_j$, zato iz vsakega vozlišča vodi natanko k različnih povezav. □

Primer 2.15. Na levi imamo sliko Cayleyjevega grafa diedrske grupe $D_{10} = \langle r, Z \rangle$, generiranega z množico $\{r, r^4, Z\}$. Na desni imamo sliko Cayleyjevega grafa proste grupe $F_2 = \langle a, b \rangle$, generiranega z množico $\{a^{\pm 1}, b^{\pm 1}\}$. Slika je prosto dostopna na spletu [24], na njej je enota 1_{F_2} označena z e. Celotnega grafa seveda ne moremo smiselno narisati na sliko, saj so po trditvi 2.7 proste grupe torzijsko proste, zato imajo neskončno elementov.



Slika 1: Graf $\mathrm{Cay}(D_{10}, \{r, r^4, Z\})$.



Slika 2: Graf $\mathrm{Cay}(F_2, \{a^{\pm 1}, b^{\pm 1}\})$.

♢

Definicija 2.16. Številu

$$\alpha_k(G) := \min \{ l(w) |\, w \in F_k \setminus \{1\} \text{ je zakon v } G \} \cup \{\infty\}$$

rečemo *k-črkovna ožina grupe G.*

Opomba 2.17. Ime ožina grupe – ki je uporabljeno na primer v virih [17], [4] in [16] – je nekoliko zavajajoče. Izhaja iz Cayleyjevega grafa grupe, vsak njegov cikel $g_1, g_2, \ldots, g_n, g_1$ namreč podaja zvezo $s_1 s_2 \cdots s_n = 1_G$ za elemente $s_i \in S$, kjer za $i = 2, \ldots, n$ velja $s_i = g_{i-1}^{-1} g_i$ in $s_1 = g_n^{-1} g_1$. V kontekstu zakonov je to ime do neke mere neupravičeno, saj beseda $s_1 s_2 \cdots s_n$ ni nujno zakon v grupi. Če si pogledamo na primer grupo $C_3 \times C_5 = \langle (\xi, 1), (1, \eta) \rangle$, bo Cayleyjev graf $\mathrm{Cay}(C_3 \times C_5, \{(\xi, 1)^{\pm 1}, (1, \eta)^{\pm 1}\})$ vseboval 3-cikel, ki ga porodi generator $(\xi, 1)$. Po drugi strani pa beseda ξ^3 očitno ni zakon v grupi $C_3 \times C_5$, ki premore element reda 5. Ker je grupa $C_3 \times C_5$ Abelova, ni težko razmisliti, da velja $\alpha_k(C_3 \times C_5) = 4$ za $k \geq 2$ in $\alpha_1(C_3 \times C_5) = 15$.

Izkaže se, da so najbolj zanimivi in za obravnavo relevantni dvočrkovni zakoni. To nam sporočata naslednji dve trditvi, ki ju najdemo v [17, str. 5].

Trditev 2.18. *Obstaja vložitev grupe $F_{2 \cdot 3^k} = \langle a_1, \ldots, a_{2 \cdot 3^k} \rangle$ v grupo $F_2 = \langle a, b \rangle$, tako da velja $l(a_i) = 2k + 1$. Tu smo z $l(w)$ označili dolžino besede $w \in F_2 = \langle a, b \rangle$.*

Dokaz. Dokaz trditve ni posebno zahteven, vendar je nekoliko preveč tehničen za naše potrebe, saj bi zahteval uvedbo in razumevanje pojmov Schreierjevega grafa ter fundamentalne grupe grafa, ki ju tekom naloge sicer ne potrebujemo. Naveden je v [17, str. 5], glavna ideja je obravnavati Cayleyev graf proste grupe F_2 z dvema generatorjema. Drevo vseh besed dolžine k na ustrezen način dopolnimo (do Schreierjevega grafa) tako, da dodamo povezave listom. Pri tem dobimo cikle dolžine $2k + 1$ in (s pomočjo fundamentalne grupe grafa) utemeljimo, da lahko jih lahko obravnavamo kot elemente $F_{2 \cdot 3^k}$, vložene v F_2. □

Posledica 2.19. *Naj bo G grupa in $k \geq 2$ naravno število. Potem velja*

$$\alpha_k(G) \leq \alpha_2(G)$$

in

$$\alpha_2(G) \leq \left(2 \left\lceil \log_3 \left(\frac{k}{2} \right) \right\rceil + 1 \right) \alpha_k(G).$$

Dokaz. Prva neenakost je očitna, saj so vsi dvočrkovni zakoni tudi k-črkovni zakoni. Druga neenakost drži, saj lahko po prejšnji trditvi vložimo $F_{2 \cdot 3^{\lceil \log_3 (\frac{k}{2}) \rceil}}$ v F_2 tako, da noben generator ni daljši od $2 \cdot 3^{\lceil \log_3 (\frac{k}{2}) \rceil} + 1$. Hkrati velja $F_k \subseteq F_{2 \cdot 3^{\lceil \log_3 (\frac{k}{2}) \rceil}}$, kar nam da želeno neenakost. □

2.3 Praštevilski izrek

V razdelku bomo spoznali praštevilski izrek ter dokazali nekaj njegovih posledic, ki bodo igrale pomembno vlogo pri obravnavi grup $\mathrm{PSL}_2(q)$ v razdelku 5.2. Pred formulacijo moramo uvesti nekaj definicij.

Definicija 2.20. Naj bosta $f, g : \mathbb{N} \to \mathbb{R}$ funkciji. Pravimo, da je funkcija f *razreda* $o(g)$, če velja $\lim_{n \to \infty} f(n)/g(n) = 0$. Poleg tega rečemo, da je *razreda* $O(g)$, če obstaja takšna konstanta $C > 0$, da za vsa dovolj velika števila n velja $f(n) \leq Cg(n)$. V tem kontekstu bomo razumeli, da je $f \in o(1)$, če velja $\lim_{n \to \infty} f(n) = 0$ in $f \in O(1)$, če obstaja konstanta $C > 0$, da je $f(n) < C$ za vsa dovolj velika števila n.

Definicija 2.21. Naj bosta $f, g : \mathbb{N} \to \mathbb{R}$ funkciji, pri čemer naj g nima ničel od nekega števila dalje. Pravimo, da sta f in g *asimptotsko ekvivalenti*, če velja

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

V tem primeru označimo $f \sim g$.

Opomba 2.22. Če sta funkciji f in g asimptotsko ekvivalentni, velja zveza $f(n) = (1 + o(1))g(n)$.

Dokaz. Obstaja neko naravno število N_1 z lastnostjo, da za vsak $n \geq N_1$ velja $g(n) \neq 0$. Zato lahko za $n \geq N_1$ zapišemo

$$\frac{f(n)}{g(n)} = 1 + h(n).$$

Po definicji asimptotske ekvivalence sledi, da je $\lim_{n\to\infty} h(n) = 0$, torej je $h \in o(1)$. □

Definicija 2.23. Definirajmo funkciji $\pi, \tau : \mathbb{R} \to \mathbb{N} \cup \{0\}$, ki preštejeta število praštevil oziroma praštevilskih potenc do vključno nekega števila:

$$\pi(x) := \sum_{p\leq x,\, p\in\mathbb{P}} 1 \quad \text{in} \quad \tau(x) := \sum_{p^k\leq x,\, k\geq 1,\, p\in\mathbb{P}} 1.$$

Izrek 2.24 (Praštevilski izrek)**.** *Za funkciji π in τ iz definicije 2.23 veljata asimptotski ekvivalenci*

$$\pi(x) \sim \frac{x}{\log x} \quad \textit{in} \quad \tau(x) \sim \frac{x}{\log x}.$$

Zgodovina praštevilskega izreka sega v konec 18. stoletja, ko je petnajstletni Gauss na podlagi empričnih vrednosti domneval, da mora veljati zveza $\pi(x) \sim x/\log x$ ([14, str. 1]). Tekom svojega življenja mu domneve ni uspelo dokazati, dočakal pa je preboj, ki ga je leta 1851 izvedel Čebišov z uvedbo funkcij θ in ψ ([8, str. 4–5]).

Definicija 2.25 (Funkciji Čebišova)**.** Funkcijama $\theta, \psi : \mathbb{R} \to \mathbb{R}$ s predpisoma

$$\theta(x) := \sum_{p\leq x,\, p\in\mathbb{P}} \log(p) \quad \text{in} \quad \psi(x) := \sum_{p^k\leq x,\, k\geq 1,\, p\in\mathbb{P}}$$

rečemo *funkciji Čebišova.*

Izrek 2.26 (Čebišov)**.** *Veljata zvezi*

$$\pi(x) \sim \frac{x}{\log x} \iff \theta(x) \sim x \quad \textit{in} \quad \tau(x) \sim \frac{x}{\log x} \iff \psi(x) \sim x.$$

Dokaz. Dokaz najdemo v [14, str. 4]. Pokažimo le zvezo $\pi(x) \sim \frac{x}{\log x} \iff \theta(x) \sim x$, dokaz druge je praktično enak. Očitno veljata neenakosti

$$0 \leq \theta(x) = \sum_{p\leq x,\, p\in\mathbb{P}} \log(p) \leq \pi(x) \log x.$$

Od tod za $x > 0$ sledi

$$\frac{\theta(x)}{x} \leq \frac{\pi(x)\log x}{x}. \tag{2.1}$$

Za vsako število $\varepsilon \in (0,1)$ imamo

$$\begin{aligned}\theta(x) \geq \sum_{x^{1-\varepsilon}<p\leq x,\, p\in\mathbb{P}} \log p &\geq (\log x^{1-\varepsilon})\left(\pi(x) - \pi(x^{1-\varepsilon})\right) \\ &= (1-\varepsilon)(\log x)\left(\pi(x) - \pi(x^{1-\varepsilon})\right) \\ &\geq (1-\varepsilon)(\log x)(\pi(x) - x^{1-\varepsilon}).\end{aligned}$$

Od tod sledi

$$\pi(x) \leq \left(\frac{1}{1-\varepsilon}\right)\frac{\theta(x)}{\log x} + x^{1-\varepsilon}. \tag{2.2}$$

Z upoštevanjem neenakosti 2.1 in 2.2 za vsako število $\varepsilon \in (0,1)$ dobimo oceno

$$\frac{\theta(x)}{x} \leq \frac{\pi(x)\log x}{x} \leq \left(\frac{1}{1-\varepsilon}\right)\frac{\theta(x)}{x} + \frac{\log x}{x^{\varepsilon}}.$$

Ker člen $\log x/x^{\varepsilon}$ konvergira proti 0 ko pošljemo $x \to \infty$, sta kvocienta $\theta(x)/x$ in $\pi(x)\log x/x$ poljubno blizu za dovolj velike x. Če eden izmed njiju konvergira proti 1, mora tudi drugi. □

Poleg zgornjega izreka je Čebišev leta 1851 dokazal ([8, str. 4–5]), da limita $\pi(x)\log x/x$ – če le obstaja – mora biti enaka 1. Naslednji preboj je uspel Riemannu v svojem znamenitem članku [15] leta 1859, v katerem je povezal porazdeltev praštevil s funkcijo zeta in formuliral prvo obliko hipoteze, ki dandanes nosi njegovo ime. Leta 1896 sta praštevilski izrek naposled neodvisno dokazala Hadamard in De la Vallée Poussin z upoštevanjem Riemannovih ugotovitev.

Skico dokaza praštevilskega izreka 2.24, ki jo bomo predstavili v nalogi, je podal Newman leta 1980. Opisana je v viru [14, str. 9].

Skica dokaza. Najprej moramo pokazati, da za nepadajočo funkcijo $f : \mathbb{R}_{\geq 1} \to \mathbb{R}$ velja sklep

$$\int_1^{\infty} \frac{f(t)-t}{t^2}\,dt \text{ konvergira} \implies f(x) \sim x.$$

Nato uvedemo funkcijo $H(t) := \theta(e^t)e^{-t} - 1$, ki je kosoma zvezna in omejena. Z uporabo lastnosti holomorfnih funkcij ugotovimo, da integral

$$\int_0^{\infty} H(t)\,dt = \int_0^{\infty} (\theta(e^t)e^{-t} - 1)\,dt \overset{t\mapsto\log x}{=} \int_1^{\infty} \frac{\theta(x)-x}{x^2}\,dx$$

konvergira. Ker je θ nepadajoča funkcija, sledi $\theta(x) \sim x$, kar je po izreku Čebišova 2.26 ekvivalentno praštevilskemu izreku $\pi(x) \sim x/\log x$. □

Za konec dokažimo še oceno, ki smo jo napovedali v uvodu. Ponovno jo bomo uporabili v razdelku 5.1.

Lema 2.27. *Velja ocena*

$$\operatorname{lcm}(1,\ldots,n) \sim \exp(n).$$

Dokaz. Po definicji najmanjšega skupnega večkratnika velja

$$\operatorname{lcm}(1,\ldots,n) = \prod_{p^k \leq n,\, p^{k+1} > n,\, p\in\mathbb{P},\, k\geq 1} p^k.$$

Z logaritmiranjem te enačbe in uporabo funkcij Čebišova 2.25 dobimo oceni

$$\theta(n) = \sum_{p\leq n,\, p\in\mathbb{P}} \log(p) \leq \log(\operatorname{lcm}(1,\ldots,n)) \leq \sum_{p^k\leq n,\, p\in\mathbb{P},\, k\geq 1} \log(p^k) = \psi(n).$$

Po Čebišovi formulaciji praštevilskega izreka 2.26 in izreku o sendviču sledi

$$\lim_{n\to\infty} \frac{\log(\operatorname{lcm}(1,\ldots,n))}{n} = 1.$$

Od tod sledi želena ocena

$$\operatorname{lcm}(1,\ldots,n) \sim \exp(n).$$

□

3 Komutatorska in razširitvena lema

3.1 Komutatorska lema

Recimo, da poznamo zakone v nekaterih podmnožicah grupe G, zanima pa nas, kako bi iz njih zgradili zakone v večjih podmnožicah te grupe. Na to vprašanje odgovarjata komutatorska in razširitvena lema, ki sta ključni orodji pri obravnavi zakonov. Začeli bomo z dokazom komutatorske leme, za katerega bomo potrebovali nekaj definicij.

Definicija 3.1. Naj bo G grupa in $w \in F_k$. Potem množico

$$Z(G,w) := \left\{(g_1,..,g_k) \in G^k \middle| \, w(g_1,\ldots,g_k) = 1_G\right\}$$

imenujemo *izginajoča množica besede w v grupi G*. Tu $w(g_1,\ldots,g_k)$ označuje evalvacijo besede w z elementi $g_1,\ldots,g_n$, v skladu z notacijo na začetku razdelka 2.2.

Lema 3.2. *Naj bosta $w_1, w_2 \in F_2 = \langle a,b\rangle$ besedi. Potem velja natanko ena izmed naslednjih trditev.*

1. *Besedi w_1 in w_2 komutirata in imata isto osnovo: Obstaja element $c \in F_2$ ter števili $k_1, k_2 \in \mathbb{Z}$, da velja $w_1 = c^{k_1}$ in $w_2 = c^{k_2}$.*
2. *Podgrupa $\langle w_1, w_2\rangle \subseteq F_2$ je izomorfna prosti grupi F_2.*

Dokaz. Po Nielsen–Schreierjevem izreku 2.8 vemo, da je $F := \langle w_1, w_2\rangle \leq F_2$ prosta grupa. Preslikava $\varphi : F_2 = \langle a,b\rangle \to F$, inducirana s slikama $a \mapsto w_1$, $b \mapsto w_2$, je očitno epimorfizem. Od tod po trditvi 2.4 sledi, da je F generirana z enim ali dvema elementoma. V prvem primeru je $F = \langle c\rangle$ za neko besedo $c \in F_2$, od koder sledi $w_1 = c^{k_1}$ in $w_2 = c^{k_2}$ za neki celi števili k_1 in k_2. V tem primeru besedi w_1 in w_2 očitno komutirata. V drugem primeru je F po trditvi 2.4 izomorfna prosti grupi F_2. □

Preden se lotimo komutatorske leme, uvedimo še naslednjo definicijo.

Definicija 3.3. Naj bo G grupa. Element $g \in G$ je *periodičen*, če je oblike $g = h^n$ za neki element $h \in G$ in število $n \in \mathbb{Z} \setminus \{0, \pm 1\}$. Sicer rečemo, da je g *aperiodičen*.

Osnovna ideja komutatorske leme je pravzaprav preprosta. Recimo, da imamo besedi $w_1, w_2 \in F_2 \setminus \{1_{F_2}\} = \langle a,b\rangle$, ki jima pripadata izginjajoči množici $Z(G,w_1)$ ter $Z(G,w_2)$. Oglejmo si komutator $w = [w_1, w_2]$. Če vzamemo par $(g,h) \in Z(G,w_1)$, bo veljalo

$$w(g,h) = [w_1(g,h), w_2(g,h)] = [1_{F_2}, w_2(g,h)] = 1_{F_2}.$$

Seveda velja simetrično tudi za pare druge izginjajoče množice. Od tod sledi sklep

$$Z(G,[w_1,w_2]) \supseteq Z(G,w_1) \cup Z(G,w_2).$$

Glavni problem, na katerega lahko naletimo pri takšnem združevanju besed, je potencialna trivialnost komutatorja $[w_1, w_2]$, ki bi ustrezala trivialnemu zakonu. Po lemi 3.2 je komutator $[w_1, w_2]$ trivialen natanko tedaj, ko sta besedi w_1 in w_2 periodični z isto osnovo. Komutatorska lema podaja konstrukcijo, ki preprečuje pojav takšnih zapletov. V sledeči obliki se pojavi v članku [12] in magistrskem delu [17], po katerem so prirejeni dokazi.

Lema 3.4. *Naj bo $k \geq 2$, $e \in \mathbb{N}$ in naj bodo besede $w_1, \ldots, w_m \in F_k$ netrivialne, pri čemer je $m = 2^e$. Potem obstaja aperiodična beseda $w \in F_k$ dolžine*

$$l(w) \leq 2m \left(m + \sum_{i=1}^{m} l(w_i) \right),$$

da za vsako grupo G velja

$$Z(G, w) \supseteq Z(G, w_1) \cup \ldots \cup Z(G, w_m).$$

Dokaz. Dokaz poteka z indukcijo po $e \in \mathbb{N}$. Naj bo $F_k = \langle a_1, \ldots, a_k \rangle = \langle S \rangle$. Za $e = 0$ (oziroma $m = 1$) vzamemo $w = [s, w_1]$, kjer je $s \in S$ takšna črka, da beseda w_1 ni periodična z osnovo s. To lahko zaradi pogoja $k \geq 2$ vedno storimo. Netrivialni komutator je v splošnem aperiodična beseda, kot je prvi opazil Schützenberger v članku [18] med obravnavo enačb v prostih grupah. Zato je beseda $[s, w_1]$ aperiodična dolžine največ $2(l(w_1) + 1)$. Kot smo videli v predhodnem razmisleku, za poljubno grupo G velja $\mathrm{Z}(G, w) \supseteq \mathrm{Z}(G, s) \cup \mathrm{Z}(G, w_1)$.

Zdaj se lotimo indukcijskega koraka v primeru $e \geq 1$ oziroma $m \geq 2$. Naj bodo podane besede $w_1, \ldots, w_{m/2}, w_{m/2+1}, \ldots, w_{2m}$. Po indukcijski predpostavki obstajata aperiodični besedi $v_1, v_2 \in F_k$, da velja

$$l(v_1) \leq m \left(\frac{m}{2} + \sum_{i=1}^{m/2} l(w_i) \right), \quad l(v_2) \leq m \left(\frac{m}{2} + \sum_{i=m/2+1}^{m} l(w_i) \right)$$

in

$$\mathrm{Z}(G, v_1) \supseteq \mathrm{Z}(G, w_1) \cup \ldots \cup \mathrm{Z}(G, w_{m/2}),$$
$$\mathrm{Z}(G, v_2) \supseteq \mathrm{Z}(G, w_{m/2+1}) \cup \ldots \cup \mathrm{Z}(G, w_m)$$

za vsako grupo G.

Zdaj moramo le še ugotoviti, kako lahko besedi v_1 ter v_2 ustrezno združimo. Po lemi 3.2 vemo, da bo komutator $[v_1, v_2]$ trivialen natanko v primeru $v_1 = v_2^{\pm 1}$, ker sta v_1 in v_2 po predpostavki aperiodični. V tem primeru imamo

$$\mathrm{Z}(G, w_1) = \mathrm{Z}(G, w_2)$$

in lahko nastavimo $w := v_1$ ali $w := v_2$, pri čemer je pogoj na dolžino besede w očitno izpolnjen. Če imamo $v_1 \neq v_2^{\pm 1}$, nastavimo $w := [v_1, v_2] \neq 1_{F_k}$. Netrivialni komutatorji so aperiodične besede po [18]. Indukcijska predpostavka nam zagotavlja

$$l(w) \leq 2m \left(\frac{m}{2} + \sum_{i=1}^{m/2} l(w_i) \right) + 2m \left(\frac{m}{2} + \sum_{i=m/2+1}^{m} l(w_i) \right) = 2m \left(m + \sum_{i=1}^{m} l(w_i) \right).$$

□

Lemo brez težav posplošimo tudi na število besed, ki ni dvojiška potenca.

Lema 3.5. *Naj bo $k \geq 2$ in naj bodo podane netrivialne besede $w_1, \ldots, w_m \in F_m$. Potem obstaja aperiodična beseda $w \in F_k$ dolžine*

$$l(w) \leq 8m \left(m + \sum_{i=1}^{m} l(w_i) \right),$$

da za vsako grupo G velja

$$\mathrm{Z}(G, w) \supseteq \mathrm{Z}(G, w_1) \cup \ldots \cup \mathrm{Z}(G, w_m).$$

Dokaz. Naj bo e takšno naravno število, da velja $m \leq 2^e < 2m$. Nastavimo

$$w_1' := w_1, \ldots, w_m' := w_m, w_{m+1}' := w_1, \ldots, w_{2^e}' := w_{2^e-m}.$$

Ker velja $m < 2m$ in $\sum_{i=1}^{2^e} w_i' \leq 2\sum_{i=1}^{m} l(w_i)$, želena ocena sledi z uporabo leme 3.4. □

Ta rezultat lahko nekoliko omilimo, da dobimo bolj praktično oceno.

Posledica 3.6. *Naj bo $k \geq 2$ in naj bodo podane netrivialne besede $w_1, \ldots, w_m \in F_k$. Potem obstaja aperiodična beseda $w \in F_k$ dolžine*

$$l(w) \leq 8m^2 \left(1 + \max_{i=1,\ldots,m} l(w_i)\right),$$

da za vsako grupo G velja

$$\mathrm{Z}(G, w) \supseteq \mathrm{Z}(G, w_1) \cup \ldots \cup \mathrm{Z}(G, w_m).$$

Dokaz. To je direktna posledica leme 3.5 skupaj z dejstvom, da je

$$\sum_{i=1}^{m} l(w_i) \leq m \max_{i=1,\ldots,m} l(w_i).$$

□

Primer 3.7. Naj bo G grupa. Recimo, da red vsakega njenega elementa deli vsaj eno izmed naravnih števil $n_1 \ldots, n_m$. Če za vsak $i = 1, \ldots, m$ uvedemo množico $H_{n_i} := \{g \in G | g^{n_i} = 1_G\}$, očitno velja, da je $\bigcup_{i=1}^{m} H_{n_i} = G$. Ker za vsak i velja $Z(G, a^{n_i}) = H_{n_i} \times G$, lahko s pomočjo komutatorske leme 3.6 združimo besede a^{n_i} v besedo w dolžine

$$l(w) \leq 8m^2 \left(1 + \max_{i=1,\ldots,m} n_i\right),$$

ki je zakon v grupi G, saj velja

$$Z(G, w) \supseteq \bigcup_{i=1}^{m} Z(G, a^{n_i}) = \bigcup_{i=1}^{m} H_{n_i} \times G = G \times G.$$

♢

Čeprav je ta primer razmeroma preprost, je ključen pri praktično vseh konstrukcijah zakonov, kar bomo videli recimo na koncu razdelka 5.2 pri obravnavi družine grup $\mathrm{PSL}_2(q)$.

3.2 Razširitvena lema

Nekoliko bolj povezana s strukturo grup je razširitvena lema. Za njeno formulacijo najprej definirajmo kratka eksaktna zaporedja.

Definicija 3.8. Naj bodo A, B, C grupe in naj $\mathbf{1}$ označuje trivialno grupo. Kratko eksaktno zaporedje je zaporedje homomorfizmov

$$\mathbf{1} \to A \xrightarrow{\varphi} B \xrightarrow{\psi} C \to \mathbf{1},$$

kjer je $\ker \psi = \mathrm{im}\, \varphi$, φ je injektivni in ψ surjektivni homomorfizem.

Razširitvena lema je v podobni obliki podana v [17, str. 9–10].

Lema 3.9. *Naj bo N edinka v grupi G in naj bosta $i : N \to G$ inkluzija ter $\pi : G \to G/N$ kanonična projekcija. To lahko zapišemo z naslednjim kratkim eksaktnim zaporedjem.*

$$\mathbf{1} \to N \xrightarrow{i} G \xrightarrow{\pi} G/N \to \mathbf{1}$$

Naj bo $F_k = \langle a_1, \ldots, a_k \rangle = \langle S \rangle$. Naj bo $w_N \in F_k$ netrivialni zakon v grupi N in $w_{G/N} \in F_k$ netrivialni zakon v kvocientu G/N. Potem obstaja netrivialni k-črkovni zakon v grupi G dolžine največ $l(w_N)l(w_{G/N})$.

Dokaz. Dokaz je prirejen po [17, str. 10] in obravnava dva možna primera oblike zakona $w_{G/N}$. V prvem primeru je $w_{G/N}$ enočrkovni zakon, torej je oblike $w_{G/N} = s^n$ za neko črko $s \in S$ in neničelno celo število n. V tem primeru je za vsak $i = 1, \ldots, k$ beseda a_i^n zakon v kvocientu G/N. Definirajmo besedo

$$w := w_N(a_1^n, \ldots, a_k^n).$$

Ker je za vsak $i = 1, \ldots, k$ beseda a_i^n zakon v kvocientu, preslikava $g \mapsto g^n$ vse elemente iz G slika v elemente edinke N. Ker je w_N netrivialni zakon v grupi N in med paroma različnimi besedami a_i^n ne more priti do krajšanja, je beseda w netrivialni zakon v grupi G. Enak razmislek izvedemo v primeru, ko je $w_{G/N}$ oblike $(s^n)^u$ za neko besedo $u \in F_k$, saj ga s konjugianjem prevedemo v enočrkovno obliko.

Če $w_{G/N}$ ni enočrkovni zakon ali konjugiranka enočrkovnega zakona, lahko brez škode za splošnost predpostavimo, da se začne s črko a_1. Potem ga pretvorimo v obliko $w_{G/N} = a_1 w'_{G/N} a_2$, kjer se $w'_{G/N}$ niti ne začne z a_1^{-1} niti ne konča z a_2^{-1}. z zaporednim izvajanjem enega izmed treh korakov:

- Če je zakon $w_{G/N}$ oblike $a_1 w'_{G/N} a_1$, ga konjugiramo s črko a_1 tolikokrat, da se zadnja črka razlikuje od a_1.
- Če je zakon oblike $w_{G/N}$ oblike $a_1 w'_{G/N} a_1^{-1}$, ga konjugiramo s črko a_1^{-1}, s čimer zmanjšamo problem.
- Če se zakon ne začne s črko a_1 zaradi prejšnjega koraka, izvedemo takšno bijektivno transformacijo črk, da se beseda začne z a_1 in, če je le mogoče, konča z a_2. To transformacijo nam inducira univerzalna lastnost prostih grup.

Pri tem se zavedajmo, da zakoni v grupi tvorijo karakteristično edinko proste grupe F_k (razmislek pod definicijo 2.9), zato je uporaba zgoraj naštetih transformacij legitimna. Nato definiramo besede

$$w_i := w_{G/N}(a_i, \ldots, a_k, a_1, \ldots, a_{i-1}).$$

Ni težko preveriti, da so netrivialni produkti besed w_i – torej $w_i w_j$, $w_i^{-1} w_j$, $w_i^{-1} w_j^{-1}$, $w_i w_j^{-1}$, $w_i w_i$, $w_i^{-1} w_i^{-1}$ za vse paroma različne $i, j \in \{1, \ldots, k\}$ – okrajšani. Zato je

$$w := w_N(w_1, \ldots, w_k)$$

netrivialni zakon v grupi G. Vse besede w_i namreč inducirajo preslikave, ki G slikajo v N, w_N pa je netrivialni zakon v N. □

Primer 3.10. S pomočjo razširitvene leme lakho dokažemo, da za vsak $n \in \mathbb{N}$ obstaja zakon $w \in F_2$ dolžine 8 v diedrski grupi D_{2n}. Ker ima podgrupa $\langle r \rangle \subseteq D_{2n}$ indeks 2, je edinka, zato lahko tvorimo kratko eksaktno zaporedje

$$\mathbf{1} \to \langle r \rangle \xrightarrow{i} D_{2n} \xrightarrow{\pi} D_{2n}/\langle r \rangle \to \mathbf{1}.$$

Ker je podgrupa $\langle r \rangle$ Abelova, je v njej zakon beseda $[a, b] = aba^{-1}b^{-1}$, grupa $D_{2n}/\langle r \rangle$ pa je moči 2 in je zato v njej zakon beseda a^2. Po lemi 3.9 torej obstaja beseda $w \in F_2$ dolžine $l(w) \leq 8$, ki je zakon v D_{2n}. Če sledimo konstrukciji izreka, vidimo, da je to natanko beseda $w = [a^2, b^2] = a^2b^2a^{-2}b^{-2}$. ♢

Iz primera je razvidno, da je moč razširitvene leme je še posebej izrazita, kadar ima grupa kakšno edinko z lepimi lastnosti, kot so na primer rešljivost, nilpotentnost ali celo Abelovost. Od tod sledi tudi, da so s stališča preučevanja zakonov *virtualno nilpotentne* oziroma *rešljive grupe* – torej grupe, ki imajo nilpotentno oziroma rešljivo edinko končnega indeksa – praktično enake nilpotentnim oziroma rešljivim. Naravna posledica razširitvene leme je tudi dejstvo, da bistveno vlogo pri iskanju kratkih zakonov igrajo enostavne grupe, saj lahko problem iskanja zakonov v neenostavnih grupah vedno prevedemo na dva manjša; na problema edinke in njenega kvocienta.

4 Nilpotentne in rešljive grupe

4.1 Definicija in osnovne lastnosti

Intuitivno gledano so nilpotentne in rešljive grupe tiste, ki so po svoji strukturi še najbolj podobne Abelovim. Da jih lahko vpeljemo, moramo najprej uvesti nekaj pojmov.

Definicija 4.1. Naj bo G grupa in $H, K \leq G$ njeni podgrupi. Potem definiramo *komutatorsko podgrupo H in K* kot podgrupo

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

Definicija 4.2. Naj bo G grupa in $(H_k)_{k \geq 1}$ padajoče zaporedje njenih podgrup, torej $H_{i+1} \subseteq H_i$ za vsak $i \geq 1$. Rečemo, da se *zaporedje $(H_k)_{k \geq 1}$ izteče z grupo K*, če obstaja naravno število n, da velja $H_k = K$ za vsako naravno število $k \geq n$.

Definicija 4.3. Grupa G je *nilpotentna*, če se *spodnja centralna vrsta* $(\gamma_k(G))_{k \geq 1}$, podana rekurzivno z

$$\gamma_1(G) := G \text{ in } \gamma_{k+1}(G) := [\gamma_k(G), G],$$

izteče s trivialno grupo. Najmanjšemu številu d, za katerega je $\gamma_{d+1} = \{1_G\}$, rečemo *razred nilpotentnosti grupe G.*

Na kratko razmislimo, da je vsak člen spodnje centralne vrste $\gamma_k(G)$ edinka v grupi G. Osnovna ideja premisleka je dejstvo, da lahko konjugiranje prenesemo v notranjost komutatorja: za poljubne elemente $g, h, k \in G$ velja zveza

$$[g, h]^k = kghg^{-1}h^{-1}k^{-1} = kgk^{-1}khk^{-1}kg^{-1}k^{-1}kh^{-1}k^{-1} = [kgk^{-1}, khk^{-1}] = [g^k, h^k].$$

Elementi grupe $\gamma_2(G) = [G, G]$ so po definiciji oblike $\prod_{i=1}^{n} [g_i, h_i]$ za neke elemente $g_i, h_i \in G$, zato za vsak element $k \in G$ velja

$$\left(\prod_{i=1}^{n} [g_i, h_i] \right)^k = \prod_{i=1}^{n} [g_i^k, h_i^k].$$

S tem smo dokazali, da je $\gamma_2(G)$ edinka v G, z indukcijo pokažemo enako za vse nadaljnje člene. S tem smo hkrati utemeljili tudi, da za vsako število $k \geq 1$ velja $\gamma_{k+1}(G) \trianglelefteq \gamma_k(G)$.

Celo družino primerov nilpotentnih grup nam podaja naslednja ugotovitev.

Trditev 4.4. *Vse p-grupe so nilpotentne. Natančneje, če je $|G| = p^d$ za neko naravno število $d \geq 1$, potem je G nilpotentna razreda največ d.*

Dokaz. Naj bo $|G| = p^k$. Dokaz poteka z indukcijo po k. Za $k = 1$ je grupa Abelova in zato očitno nilpotentna. Za $k \geq 2$ uporabimo posledico razredne formule, da imajo p-grupe netrivialni center. Če je $Z(G) = G$, je grupa Abelova. Sicer sta po indukcijski predpostavki grupi $Z(G)$ in $G/Z(G)$ nilpotentni. Nilpotentnost kvocienta implicira obstoj najmanjšega števila m, za katero velja $\gamma_m(G) \subseteq Z(G)$. Od tod direktno sledi, da je $\gamma_{m+1}(G) = \{1_G\}$. □

Primer 4.5. Trditev 4.4 nam sporoča, da so vse diedrske grupe oblike $D_{2\cdot 2^k}$ nilpotentne. Izkaže se, da so to tudi edine. Ni težko premisliti, da je

$$Z(D_{2m}) = \begin{cases} \{1_{D_{2m}}\}; \text{ če je } m \text{ liho,} \\ \{1_{D_{2m}}, r^{m/2}\}; \text{ če je } m \text{ sodo.} \end{cases}$$

V nadaljevanju bomo dokazali trditev 4.7, ki pravi, da so nilpotentne grupe produkti svojih p-podgrup Sylowa. Zato za vsako nilpotentno diedrsko grupo lahko zapišemo $D_{2m} = \prod_{i=1}^{n} P_{p_i}$. Od tod sledi

$$Z(D_{2m}) = \prod_{i=1}^{n} Z(P_{p_i}).$$

Ker po razredni formuli za vsako število $i = 1, \ldots, n$ praštevilo p_i deli $|P_{p_i}|$, nam preostane le možnost, da je D_{2m} 2-grupa oziroma $m = 2^k$. ♢

Pred dokazom napovedane trditve 4.7 navedimo naslednjo definicijo.

Definicija 4.6. Naj bo G grupa in H njena podgrupa. Potem podgrupi

$$N_G(H) := \{ghg^{-1} | g \in G, h \in H\}$$

rečemo *normalizator* podgrupe H v grupi G.

Trditev 4.7. *Končne nilpotentne grupe so direktni produkt svojih p-podgrup Sylowa.*

Dokaz. Dokaz je povzet po [1]. Naj bo G nilpotentna grupa. Najprej pokažimo, da iz $H \lneq G$ sledi $H \lneq N_G(H)$. To storimo z indukcijo po moči grupe G. Če je G Abelova, izjava očitno drži. Sicer je grupa G nilpotentna razreda 2 ali več, kar pomeni, da njen center ni trivialen; če je število $d \geq 1$ razred nilpotentnosti grupe G, velja

$$\gamma_{d+1} = [\gamma_d, G] = 1 \Longrightarrow \{1_G\} \neq \gamma_d \leq Z(G) \Longrightarrow Z(G) \neq \{1_G\}.$$

Zato obravnavamo dva primera. Če center $Z(G)$ ni vsebovan H, velja $H \lneq HZ(G)$ zaradi računa

$$h^{h_Z g_Z} = h_Z g_Z h g_Z^{-1} h_Z^{-1} = h_Z h h_Z^{-1} \in H \quad \text{za vse } h, h_Z \in H, g_Z \in G.$$

Predpostavimo torej, da je $Z(G) \leq H$. Potem po korespondenčnem izreku sledi, da je $H/Z(G)$ podgrupa nilpotentne grupe $G/Z(G)$. Ker center $Z(G)$ ni trivialen, uporabimo indukcijsko predpostavko na kvocientu $G/Z(G)$ in dobimo njeno podgrupo $K/Z(G)$, v kateri je $H/Z(G)$ prava edinka. Ustrezno grupo za H dobimo kot prasliko kanonične projekcije $\pi : G \to G/Z(G)$, uporabljeno na grupi $K/Z(G)$.

S pomočjo tega sklepa dokažimo, so p-podgrupe Sylowa v nilpotentni grupi G edinke. Naj bodo $p_1, \ldots, p_s$ različna praštevila, ki delijo $|G|$, in naj bo P_i poljubna p_i-podgrupa Sylowa grupe G za vsak $1 \leq i \leq s$. Naj bo brez škode za splošnost $P := P_1$ in naj bo $N := N_G(P)$. Ker je P edinka Sylowa v N, je v njej karakteristična. Od tod sledi, da je P edinka tudi v $N_G(N)$, saj je zaradi $N \lhd N_G(N)$ konjugiranje z elementom iz $N_G(N)$ avtomorfizem grupe N. Od tod sledi $N_G(N) \leq N$ oziroma $N = N_G(N)$. Po ugotovitvi iz prejšnjega odstavka dobimo $N = G$, kar pomeni, da so p-podgrupe Sylowa nilpotentnih grup edinke.

Od tod z indukcijo po moči grupe pokažemo, da lahko G zapišemo kot direktni produkt svojih p-podgrup Sylowa. Pri tem se moramo zgolj sklicati na dejstvo, da za različni praštevili p in q velja $P_p \cap P_q = \{1_G\}$. □

Posledica 4.8. *Nilpotentna grupa G moči n ali manj je razreda nilpotentnosti največ* $\lfloor \log_2(n) \rfloor$.

Dokaz. Naj bo G nilpotentna grupa moči n ali manj in naj bo d njen razred nilpotentnosti. Naj bodo števila $p_1, \ldots, p_n$ vsi različni praštevilski delitelji $|G|$. Po trditvi 4.7 je G produkt svojih p-podgrup Sylowa, torej $G = \prod_{i=1}^{n} P_{p_i}$. Po dokazu trditve 4.4 je podgrupa P_{p_i} nilpotentna razreda največ $\log_{p_i}|P_{p_i}|$. Od tod sledi

$$d \leq \max_{i=1,\ldots,n} \log_{p_i}|P_{p_i}| \leq \left\lfloor \max_{i=1,\ldots,n} \log_2|P_{p_i}| \right\rfloor \leq \lfloor \log_2|G| \rfloor \leq \lfloor \log_2(n) \rfloor .$$

□

Definicija 4.9. Grupa G je *rešljiva*, če se *izpeljana vrsta* $(G^{(k)})_{k\geq 0}$, podana rekurzivno z

$$G^{(0)} := G \text{ in } G^{(k+1)} := [G^{(k)}, G^{(k)}],$$

izteče s trivialno grupo. Najmanjšemu številu d, za katerega je $G^{(d)} = \{1_G\}$, rečemo *razred rešljivosti grupe* G.

Analogno kot pri nilpotentnih grupah sklepamo, da izpeljana vrsta $(G^{(k)})_{k\geq 0}$ tvori verigo edink, ki so vse hkrati tudi edinke v G.

Primer 4.10. Diedrske grupe D_{2n} so rešljive razreda največ 2. Z računom je enostavno pokazati, da je $(D_{2n})^{(1)}$ podmnožica Abelove podgrupe $\langle r \rangle$, zato bo grupa $(D_{2n})^{(2)} = ((D_{2n})^{(1)})^{(1)}$ trivialna. Ta sklep namiguje na nekatere lastnosti rešljivih grup, ki jih bomo obravnavali v trditvi 4.12. ♢

Primer 4.11. Vse nilpotentne grupe so rešljive, saj velja $G^{(0)} = \gamma_1(G) = G$, z indukcijo za vsako število $k \geq 1$ sledi

$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \subseteq [\gamma_k(G), G] = \gamma_{k+1}(G).$$

Niso pa vse rešljive grupe nilpotentne, na primer diedrske grupe D_{2n}, kjer $2n$ ni dvojiška potenca. ♢

Trditev 4.12. *Za rešljive grupe veljajo naslednje osnovne lastnosti.*

1. *Vsaka podgrupa rešljive grupe je rešljiva.*
2. *Vsak kvocient rešljive grupe je rešljiv.*
3. *Naj bo $N \triangleleft G$ in naj bosta N in G/N rešljivi grupi razreda d_N oziroma $d_{G/N}$. Potem je G rešljiva grupa razreda največ $d_N + d_{G/N}$.*
4. *Naj bosta $M, N \triangleleft G$ rešljivi razreda d_M oziroma d_N. Potem je edinka MN rešljiva razreda največ $d_M + d_N$.*

Dokaz.

1. To je očitna posledica dejstva, da za $H \leq G$ velja $H^{(k)} \subseteq G^{(k)}$ za vsak $k \in \mathbb{N} \cup \{0\}$.
2. Naj bo G rešljiva in naj bo $N \triangleleft G$. Zaradi rešljivosti grupe G obstaja naravno število d, da je $G^{(k)} \subseteq N$ za vse $k \geq d$, kar implicira $(G/N)^{(k)} = \left\{1_{G/N}\right\}$ za vse $k \geq d$.

3. Ker je G/N rešljiva grupa razreda $d_{G/N}$, bo $G^{(k)} \subseteq N$ za vse $k \geq d_{G/N}$. Ker je N rešljiva razreda d_N, bo nadalje veljalo $G^{(k)} = \{1_G\}$ za vse $k \geq d_N + d_{G/N}$.

4. Dokaz je prirejen po opombi 4 iz [17, str.4]. Po drugem izreku o izomorfizmu lahko zapišemo kratko eksaktno zaporedje

$$\mathbf{1} \to M \to MN \to MN/M \cong N/(N \cap M) \to \mathbf{1}.$$

Ker je N rešljiva, je po drugi točki trditve njen kvocient $N/(N \cap M)$ rešljiv razreda največ d_N in posledično enako velja za kvocient MN/M. Ker je M rešljiva razreda d_M, po tretji točki trditve sledi $(MN)^{(k)} = \{1_G\}$ za vse $k \geq d_N + d_M$.

□

Razširitvena lema 3.9 nam ponuja naslednjo preprosto oceno dolžine kratkih netrivialnih zakonov v rešljivih oziroma nilpotentnih grupah.

Trditev 4.13. *Obstaja beseda $w \in F_2 = \langle a, b\rangle$ dolžine $l(w) \leq 4^d$, ki je zakon v vseh grupah razreda rešljivosti (ali nilpotentnosti) d ali manj.*

Dokaz. Trditev je posledica razširitvene leme 3.9, dokaz poteka z indukcijo po razredu rešljivosti grupe G, ki ga označimo z d. Za $d = 1$ je grupa G Abelova, zato je ustrezni zakon beseda $w = [a, b]$, ki je dolžine 4. Za $d > 1$ opazimo, da je kvocient $G/G^{(1)}$ Abelova grupa, $G^{(1)}$ pa rešljiva grupa razreda največ $d - 1$. Zato z uporabo razširitvene leme in indukcijske predpostavke najdemo besedo $w \in F_2$ dolžine

$$l(w) \leq 4 \cdot 4^{d-1} = 4^d,$$

ki je zakon v grupi G. Za nilpotentne grupe upoštevamo dejstvo $G^{(1)} \subseteq \gamma_2(G)$, kar implicira komutativnost grupe $G/\gamma_2(G)$ ($G^{(1)}$ je po definiciji najmanjša edinka, za katero je kvocient $G/G^{(1)}$ Abelova grupa). □

Opomba 4.14. V članku [12, str. 8] je podana nekoliko šibkejša meja $l(w) \leq 4 \cdot 6^{d-1}$, ker je avtor uporabil šibkejšo obliko razširitvene leme.

4.2 Konstrukcija zakonov v nilpotentnih in rešljivih grupah

Vemo, da je vsaka nilpotentna grupa rešljiva. Če lahko učinkovito omejimo njen razred rešljivosti, bomo s pomočjo ocene 4.13 dobili oceno dolžine kratkih zakonov v nilpotentnih grupah.

Bolj konkretno, dokazali bomo, da za vsako celo število $n \geq 0$ velja zveza med členi izpeljane in centralne vrste $G^{(n)} \subseteq \gamma_{2^n}(G)$. Ideji za dokaza lem 4.15 in 4.16 se nahajata v [17, str. 17–18].

Lema 4.15. *Naj bo G grupa, $A, B, C \trianglelefteq G$ njene edinke in $D \leq G$ njena podgrupa. Če velja*

$$[[A, B], C] \subseteq D \text{ in } [[B, C], A] \subseteq D,$$

velja tudi

$$[[C, A], B].$$

Elementi komutatorske podgrupe $[[A,B],C]$ so oblike $\prod_{i=1}^{n}[[a_i,b_i],c_i]$ za neke elemente $a_i \in A, b_i \in B, c_i \in C$. Z računom lahko preverimo, da poljubne elemente $g,h,k \in G$ velja Hall-Wittova enakost

$$[[g^{-1},h],k] = \Big(\big([[k^{-1},g],h]^{k^{-1}}[[h^{-1},k],g]^{h^{-1}}\big)^{g}\Big)^{-1}.$$

To pomeni, da lahko zapišemo

$$\prod_{i=1}^{n}[[a_i,b_i],c_i] = \prod_{i=1}^{n}\left(\left(\underbrace{[[c_i^{-1},a_i],b_i]^{c_i^{-1}}}_{\in[[C,A],B]}\underbrace{[[b_i^{-1},c_i],a_i]^{b_i^{-1}}}_{\in[[B,C],A]}\right)^{a_i}\right)^{-1}.$$

Od tod po predpostavkah sledi, da je $[[A,B],C] \subseteq [[C,A],B][[B,C],A] \subseteq D$.

Lema 4.16. *Za vsako število $n \geq 0$ velja inkluzija*

$$G^{(n)} \subseteq \gamma_{2^n}(G).$$

Dokaz. Dokaz poteka z indukcijo po n. Za $n = 0$ po definiciji velja $G^{(0)} \subseteq \gamma_1(G)$. Za $n \geq 1$ velja

$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}] \subseteq [\gamma_{2^{n-1}}(G), \gamma_{2^{n-1}}(G)].$$

Če bi uspeli dokazati, da za poljubni števili $i,j \geq 1$ velja

$$[\gamma_i(G), \gamma_j(G)] \subseteq \gamma_{i+j}(G),$$

bi dokazali lemo. Zato bomo izvedli indukcijo po številu j. V primeru $j = 1$ imamo

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

Predpostavimo, da je $j > 1$. Po indukcijski predpostavki veljata sklepa

$$[[\gamma_{j-1}(G), \gamma_i(G)], G] \overset{\text{i. p.}}{\subseteq} [\gamma_{i+j-1}(G), G] = \gamma_{i+j}(G)$$

in

$$[[\gamma_i(G), G], \gamma_{j-1}(G)] = [\gamma_{i+1}(G), \gamma_{j-1}(G)] \overset{\text{i. p.}}{\subseteq} \gamma_{i+j}(G).$$

Zato po lemi 4.15 velja

$$[\gamma_i(G), \gamma_j(G)] = [\gamma_j(G), \gamma_i(G)] = [[G, \gamma_{j-1}(G)], \gamma_i(G)] \overset{4.15}{\subseteq} \gamma_{i+j}(G).$$

Od tod sledi želena vsebovanost

$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}] \subseteq [\gamma_{2^{n-1}}(G), \gamma_{2^{n-1}}(G)] \subseteq \gamma_{2^n}(G).$$

□

Zdaj smo pripravljeni za dokaz izreka, ki predstavlja ključni razmislek, zakaj v nilpotentnih grupah obstajajo razmeroma kratki zakoni.

Izrek 4.17. *Obstaja netrivialna beseda $w \in F_2$, ki je zakon v vseh nilpotentnih grupah moči največ n, dolžine*

$$l(w) \leq 4\log_2(n)^2,$$

Dokaz. Naj bo G nilpotentna grupa moči n ali manj. Po posledici 4.8 znaša njen razred nilpotentnosti d_{nil} največ

$$d_{\text{nil}} \leq \lfloor \log_2|G| \rfloor - 1 \leq \log_2(n).$$

Po lemi 4.16 vemo tudi, da grupa razreda nilpotentnosti d_{nil} gotovo pripada razredu rešljivosti $\lceil \log_2(d_{\text{nil}}) \rceil$, oziroma $d_{\text{reš}} \leq \log_2(d_{\text{nil}})+1$ Po oceni 4.13 torej obstaja beseda $w \in F_2$ dolžine

$$l(w) \leq 4^{d_{\text{reš}}} \leq 4^{\log_2(d_{\text{nil}})+1} \leq 4 \cdot 4^{\log_2(\log_2(n))} = 4\log_2(n)^2.$$

□

Ta rezultat bi lahko izboljšali z izboljšanjem ocene 4.13 za rešljive grupe. Eden izmed možnih pristopov, ki ga najdemo recimo v [7, str. 4–5] ali [17, str. 14–16], je uvedba zaporedij $(a_n)_n$ in $(b_n)_n$ v F_2 s predpisoma

$$a_0 := a,\ a_{n+1} := [b_n^{-1}, a_n] \quad \text{in} \quad b_0 := b,\ b_{n+1} := [a_n, b_n].$$

Izkaže se, da za vsako število $n \geq 1$ besede a_n in b_n netrivialne ter velja $a_n, b_n \in F_2^{(n)}$. To pomeni, da sta za $n \geq 1$ besedi a_n in b_n netrivialna zakona v rešljivih grupah razreda n ali manj. Če grupa G ustreza tem pogojem, namreč za vsak par $g, h \in G$ velja

$$a_n(g,h), b_n(g,h) \in G^{(n)} = \{1_G\}.$$

Z indukcijo se da pokazati, da za vsako število $n \geq 0$ velja $l(a_n) = l(b_n)$, zato lahko definiramo zaporedje $c_n := l(a_n)$, ki ustreza rekurzivni formuli $c_{n+2} = 3c_{n+1} + 2c_n$ z začetnima členoma $c_0 = 1$ in $c_1 = 4$. Od tod lahko natančno izračunamo splošni člen tega zaporedja in ocenimo zgornjo mejo z zvezama

$$c_n = \left(\frac{1}{2} + \frac{5}{2\sqrt{17}}\right)\left(\frac{3+\sqrt{17}}{2}\right)^n + \left(\frac{1}{2} - \frac{5}{2\sqrt{17}}\right)\left(\frac{3-\sqrt{17}}{2}\right)^n \leq 1{,}11 \cdot 3{,}57^n + o(1),$$

kar je za $n \geq 2$ boljša ocena od 4^n iz trditve 4.13, zato nam zmanjša eksponent 2 iz izreka 4.17.

Da dobimo primerljiv rezultat za rešljive grupe, se moramo precej bolj potruditi. Postopek je opisan v [21, str. 3–4] oziroma podrobneje v [17, str. 19–25]. Sklicuje se na lastnosti grup avtomorfizmov nilpotentnih grup, ki jih vložimo v primerne splošne linearne grupe. Slednjim znamo natančno omejiti razrede rešljivosti, saj so predmet klasične obravnave v teoriji grup. Ker je jedro te vložitve nilpotentno, se lahko zaradi razširitvene leme 3.9 skličemo na rezultat o dolžinah zakonov v nilpotentnih grupah **??**, kar nam zagotovi naslednji izrek, ki ga najdemo v obliki trditve 4 v [17, str. 25].

Izrek 4.18. *Za vsako število $n \in \mathbb{N} \cup \{0\}$ obstaja netrivialna beseda $w \in F_2$ dolžine*

$$l(w) \leq (C_{10} + o(1))\log(n)^{\lambda},$$

ki je zakon v vseh rešljivih grupah moči n ali manj, kjer sta konstanti enaki $C_{10} :=$ 86.321,05422 . . . in $\lambda :=$ 4,331612776 . . .

5 Enostavne in simetrične grupe

Začnimo z razmislekom o pomembnosti enostavnih grup pri iskanju kratkih zakonov v splošnih grupah. Glavno idejo smo pravzaprav že videli v primeru 3.10, kjer smo ugotovili, da lahko problem iskanja kratkih zakonov v neki konkretni grupi prevedemo na problem o njeni edinki in kvocientu po tej edinki. Ta razčlenjevanje se ustavi pri enostavnih grupah, ki po definiciji nimajo pravih netrivialnih edink.

Ker je klasifikacija končnih enostavnih grup zaključena, lahko marsikaj povemo o njihovi strukturi. Po tej klasifikaciji obstaja 18 družin končnih enostavnih grup ter 26 sporadičnih grup ([23]), ki ne spadajo v nobeno izmed prej omenjenih družin. Za asimptotsko analizo dolžin zakonov nas sporadične grupe prav nič ne motijo. Ker so končne, vse od njih premorejo netrivialne zakone, ki jih povežemo s komutatorsko lemo 3.5 v besedo w_{spor}, ki je zakon v vseh sporadičnih grupah. Recimo, da nam s funkcijo $f(n)$ uspe omejiti dolžino besede $w_{\text{druž}}(n)$, ki je zakon v vseh grupah moči n ali manj, ki pripadajo eni izmed 18-ih družin končnih enostavnih grup. Potem s pomočjo komutatorske leme 3.4 dobimo besedo w, ki je zakon v vseh enostavnih grupah velikosti n ali manj, katere dolžina je

$$l(w) \leq 2 \cdot 2(2 + l(w_{\text{spor}}) + l(w_{\text{druž}})) \leq 4f(n) + O(1).$$

Vidimo torej, da nas pri asimptotski obravnavi zakonov sporadične grupe prav nič ne ovirajo. Omenimo še to, da iskanja kratkih zakonov v družinah končnih enostavnih grup lotimo z metodo maksimalnega reda elementov, ki je razložena v primeru 3.7. Pri tem je najbolj problematična družina grup $\mathrm{PSL}_2(q)$, katere članice imajo razmeroma visoke rede elementov glede na njihove velikosti. Ta družina grup si zaradi svojih posebnih lastnosti zasluži svoj razdelek v tem poglavju.

Morda presenetljivo se izkaže, da lahko problem iskanja kratkih zakonov v splošni končni grupi G prevedemo na problem iskanja kratkih zakonov v rešljivih, simetričnih in enostavnih grupah.

Definicija 5.1. Naj bo G končna grupa. Največjo rešljivo edinko G imenujemo *rešljivi radikal grupe* G in ga označimo z $S(G)$. Če je $S(G)$ trivialna grupa, rečemo, da je G *polenostavna grupa.*

Lema 5.2. *Rešljivi radikal je dobro definiran v končnih grupah.*

Dokaz. Naj bosta M in N rešljivi edinki končne grupe G. Po četrti točke trditve 4.12 je tudi MN rešljiva edinka (produkt edink je vedno edinka, manj očitna je rešljivost). Ker je grupa G končna, ima končno mnogo edink, s primerjanjem vseh parov v končnem številu korakov najdemo največjo. □

Lema 5.3. *Naj bo G končna grupa. Potem je kvocient $G/S(G)$ polenostavna grupa.*

Dokaz. Dokaz poteka s protislovjem. Recimo, da $G/S(G)$ ni polenostavna grupa in ima netrivialno rešljivo edinko N. Po korespondenčnem izreku je $N = N'/S(G)$ za neko edinko $N' \triangleleft G$. Ker sta tako $N'/S(G)$ kot $S(G)$ rešljivi grupi, po tretji točki trditve 4.12 sledi, da je N' rešljiva in hkrati strogo večja od $S(G)$, kar je protislovno z definicijo rešljivega radikala. □

Dokazali smo torej, da je za poljubno končno grupo G kvocient $G/S(G)$ polenostavna grupa. Izkaže se, da lahko vsako polenostavno grupo zapišemo kot produkt enostavnih grup $G/S(G) = \prod_{i=1}^{n} H_i^{k_i}$. Pri nadaljnji obravnavi polenostavnih grup pomembno vlogo igra grupa avtomorfizmov $\mathrm{Aut}\left(\prod_{i=1}^{n} H_i^{k_i}\right)$, ki jo ukrotimo s pomočjo simetričnih grup S_{k_i}. Intuitivno si lahko predstavljamo, da vsak avtomorfizem najprej permutira k_i kopij grupe H_i, nato pa še elemente v vsaki posamezni kopiji.

Dokaze omenjenih dejstev lahko najdemo v viru [21, str. 4–7] oziroma bolj podrobno v [17, str. 27–42]. Ker so preobsežni za okvir te naloge, se bomo zadovoljili z nekoliko šibkejšo oceno dolžin kratkih zakonov v splošni grupi, ki jo dobimo z vložitvijo v dovolj veliko simetrično grupo.

5.1 Simetrične grupe

V razdelku bomo najprej dokazali oceno dolžine kratkih zakonov v simetričnih grupah z uporabo praštevilskega izreka, nato pa predstavili glavni izrek članka [12], ki podaja še boljšo oceno.

S pomočjo leme 2.27 lahko ocenimo dolžine kratkih zakonov v simetričnih grupah.

Posledica 5.4. *Naj bo $n \geq 1$ naravno število. Potem obstaja beseda $w \in F_2 = \langle a, b \rangle$ dolžine*

$$l(w) = \exp\left((1 + o(1))\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\right),$$

ki je zakon v vseh grupah moči n ali manj.

Dokaz. Poljubno grupo G moči n ali manj lahko vložimo v simetrično grupo $\mathrm{Sym}(n)$, ki je moči $n!$. Po Strilingovi formuli velja

$$n! = (1 + o(1))\sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

V uvodnem razdelku smo ugotovili, da je $a^{\exp(\mathrm{Sym}(n))} = a^{\mathrm{lcm}(1,\ldots,n)}$ zakon v simetrični grupi $\mathrm{Sym}(n)$. Zato po lemi 2.27 obstaja netrivialna beseda $w = a^{\mathrm{lcm}(1,\ldots,n)} \in F_2$ dolžine

$$l(w) = \exp\left((1 + o(1))\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\right),$$

ki je zakon v vseh grupah moči n ali manj. □

Avtorja članka [12] sta rezultat močno izboljšala.

Izrek 5.5 (Kozma–Thom)**.** *Naj bo $n \geq 1$ naravno število. Potem obstajata število $C > 0$ in beseda $w \in F_2$ dolžine*

$$l(w) \leq \exp(O(1)\log(n)^4 \log(\log n)),$$

ki je zakon v simetrični grupi $\mathrm{Sym}(n)$*.*

Dokaz tega izreka preveč specifičen za potrebe te naloge, saj se močno sklicuje na posledice klasifikacije končnih enostavnih grup. Zato zgolj predstavimo glavno idejo.

Za vsako število $k \leq n$ sta avtorja najprej razdelila pare $(\sigma, \tau) \in \mathrm{Sym}(k)^2$ na tiste, ki generirajo grupo $\mathrm{Sym}(k)$, in tiste, ki generirajo preostale vrste podgrup.

S $P(k)$ sta označila množico k-ciklov v grupi $\mathrm{Sym}(k)$. Z opazovanjem naključnih sprehodov po Cayleyjevem grafu $\mathrm{Cay}(\mathrm{Sym}(k), \{\sigma^{\pm 1}, \tau^{\pm 1}\})$ sta avtorja sklepala, da obstaja kratka netrivialna beseda $w_{k,(\sigma,\tau)} \in F_2$, za katero velja $w_{k,(\sigma,\tau)}(\sigma, \tau) \in P(k)$. Od tod seveda sledi $w_{k,(\sigma,\tau)}(\sigma, \tau)^k = 1_{F_2}$. Nato sta avtorja s pomočjo komutatorske leme 3.5 vse besede $w_{k,(\sigma,\tau)}$ združila v netrivialno besedo $w_1 \in F_2$, ki je zakon v podmnožici parov elementov $\mathrm{Sym}(k)^2$, ki generirajo grupo $\mathrm{Sym}(k)$.

Za vse pare $(\sigma, \tau) \in \mathrm{Sym}(k)^2$, ki ne generirajo grupe $\mathrm{Sym}(k)$. Nato sta z uporabo komutatorske leme konstruirala netrivialno besedo $w_2 \in F_2$, ki je zakon v vseh možnih oblikah podgrupe $\langle \sigma, \tau \rangle \subsetneq \mathrm{Sym}(k)$. Na koncu sta z uporabo komutatorske leme povezala besedi w_1 in w_2 v besedo w, ki izniči tako pare, ki generirajo $\mathrm{Sym}(n)$, kot tiste, ki generirajo pravo podgrupo. Zato je beseda w zakon v grupi $\mathrm{Sym}(n)$.

Posledica 5.6. *Naj bo $n \geq 1$ naravno število. Potem obstaja beseda $w \in F_2$ dolžine*

$$l(w) \leq \exp\Big(O(1)n^4 \log(n)^4 \log(n \log(n))\Big),$$

ki je zakon v vseh grupah moči n ali manj.

Dokaz. Poljubno grupo G moči n ali manj lahko vložimo v simetrično grupo $\mathrm{Sym}(n)$, ki je moči $n!$. Po Stirlingovi formuli imamo zvezo

$$\log(n!) = \log\left((1 + o(1))\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\right) \leq (1 + o(1))n \log(n).$$

Od tod z uporabo prejšnjega izreka dobimo besedo $w \in F_2$, ki je zakon v grupi G, dolžine

$$\begin{aligned} l(w) &\leq \exp\Big(O(1) \log(n!)^4 \log(\log(n!))\Big), \\ &\leq \exp\Big(O(1)((1 + o(1))n \log(n))^4 \log((1 + o(1))n \log(n))\Big), \\ &\leq \exp\Big(O(1)n^4 \log(n)^4 \log(n \log(n))\Big). \end{aligned}$$

□

5.2 Grupe $\mathrm{PSL}_2(q)$

Tekom tega poglavja bo p vedno označevalo praštevilo, q pa praštevilsko potenco oblike $q = p^k$ za neko naravno število $k \geq 1$. Začnimo z definicijo družine grup $\mathrm{PSL}_n(q)$.

Definicija 5.7. Naj bo $n \in \mathbb{N}$ in $q \in \mathbb{N}$ praštevilska potenca, torej $q = p^k$. Potem definiramo grupo

$$\mathrm{PSL}_n(q) := \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q)).$$

V primeru $n = 2$ so elementi podgrupe $Z(\mathrm{SL}_n(q))$ skalarne 2×2 matrike z lastnostjo $\det \lambda I = 1_{\mathbb{F}_q}$. To enačbo prevedemo na enačbo oblike $(\lambda - 1)(\lambda + 1) = 0$. Če ima polje $\mathbb{F}_q$ karakteristiko 2 – kar se zgodi natanko v primeru $q = 2^k$ – sta $\lambda_{1,2} = \pm 1$ isti element, sicer pa dva različna. Tako dobimo

$$\mathrm{PSL}_2(q) = \begin{cases} \mathrm{SL}_2(q); & p = 2, \\ \mathrm{SL}_2(q)/\{I, -I\}; & p \neq 2. \end{cases}$$

Družina $\mathrm{PSL}_2(q)$ ima – poleg svoje problematičnosti pri iskanju kratkih zakonov – zelo posebne lastnosti. Ena izmed glavnih je sledeča.

Trditev 5.8. *Naj bo p praštevilo. Potem ima vsak netrivialni zakon v grupi $\mathrm{PSL}_2(p)$ dolžino vsaj p. Posledično enako velja za grupi $\mathrm{GL}_2(p)$ in $\mathrm{SL}_2(p)$, saj se zakoni prenašajo na podgrupe in kvociente.*

Dokaz. Dokaz je prirejen po [17, str. 38–39]. Glavna ideja je pokazati, da lahko z vstavljanjem matrik strižnih transformacij iz kolobarja $M_2(\mathbb{F}_p)$ v primeru prekratkih besed vedno dobimo matriko, ki ni skalarna. Tekom dokaza naj 0 označuje enoto za seštevanje, 1 pa enoto za množenje v polju $(\mathbb{F}_p, +, \cdot)$. Naj bo $w \in F_2 = \langle a, b\rangle$ beseda dolžine $l(w) < p$. Na enak način kot v dokazu razširitvene leme 3.9 ločimo dva primera.

V prvem je beseda w konjugiranka besede a^n ali b^n za neko število $n < p$. Zato lahko brez škode za splošnost predpostavimo, da je $w = a^n$. Če definiramo matriko

$$A := \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

dobimo

$$w(A, I) = A^n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} \neq \lambda I.$$

V drugem primeru je beseda w brez škode za splošnost konjugiranka besede $w = a^{r_1}b^{s_1} \cdots a^{r_k}b^{s_k}$ za neka neničelna cela števila r_i ter s_i. Pri tem mora veljati $l(w) = \sum_{i=1}^{k} |r_i| + |s_i| < p$. Nato definiramo matriki

$$B := \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix} \text{ in } C := \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}.$$

Z indukcijo po številu k pokažimo, da za besedo w velja

$$w(B, C) = \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} + r_1 s_1 \cdots r_k s_k x^{2k} \end{bmatrix},$$

kjer so polinomi $f_{12}, f_{21}, f_{22} \in \mathbb{F}_p[x]$ stopnje največ $2k - 1$, polinom $f_{11} \in \mathbb{F}_p[x]$ pa stopnje največ $2k - 2$.

Za $k = 1$ imamo

$$w(B, C) = \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}^{r_1} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{s_1} = \begin{bmatrix} 1 & s_1 x \\ r_1 x & r_1 s_1 x^2 \end{bmatrix},$$

kar nam podaja bazo indukcije. Za $k \geq 2$ izvedemo indukcijski korak na besedi $w = a^{s_0}b^{r_0}a^{s_1}b^{r_1} \cdots a^{s_k}b^{r_k}$. Tako dobimo

$$\begin{aligned} w(B, C) &= \begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}^{r_0} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{s_0} \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} + r_1 s_1 \cdots r_k s_k x^{2k} \end{bmatrix} \\ &= \begin{bmatrix} 1 & s_0 x \\ r_0 x & 1 + r_0 s_0 x^2 \end{bmatrix} \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} + r_1 s_1 \cdots r_k s_k x^{2k} \end{bmatrix} \\ &= \begin{bmatrix} f_{11} + s_0 x f_{21} & f_{12} + s_0 x (f_{22} + r_1 s_1 \cdots r_k s_k x^{2k}) \\ r_0 x f_{11} + (1 + r_0 s_0 x^2) f_{21} & r_0 x f_{12} + (1 + r_0 s_0 x^2)(f_{22} + r_1 s_1 \cdots r_k s_k x^{2k}) \end{bmatrix}. \end{aligned}$$

Po indukcijski predpostavki je f_{11} stopnje največ $2k-2$, f_{12}, f_{21} ter f_{22} pa največ $2k-1$.

Razlika diagonalnih elementov $d := -f_{11} + f_{22} + r_1 s_1 \cdots r_k s_k x^{2k}$ je polinom stopnje $1 \leq \deg(d) \leq p$. Desna neenakost sledi iz dejstva $\sum_{i=1}^{k} |r_i| + |s_i| < p$. Preostane nam le še dokazati, da lahko najdemo takšen element $u \in \mathbb{F}_p$, da bo $d(x) \neq 0$, torej matrika $w(B, C)$ ne more biti skalarna. Če bi za vse elemente $u \in \mathbb{F}_p$ veljalo $d(u) = 0$, bi lahko zapisali

$$d(x) = \alpha \prod_{u \in \mathbb{F}_p} (x - u), \;\; \alpha \in \mathbb{F}_p^*,$$

ker vemo, da d ni ničelni polinom. Zaradi pogoja $\deg(d) < p$ ima lahko polinom d največ $p-1$ različnih ničel, zato nas zgornji zapis vodi do protislovja. To pomeni, da obstaja element $x \in \mathbb{F}_p$, za katerega beseda $w(B, C)$ ni skalarna matrika in posledično w ne more biti zakon v grupi $\mathrm{PSL}_2(p)$.

□

Direktna posledica te leme je recimo dejstvo, da grupa $\mathrm{Sym}(\mathbb{N})$ nima netrivialnih zakonov, saj vsebuje vse $\mathrm{PSL}_2(p)$ kot podgrupe. Še bolj očiten primer grupe, ki nima dvočrkovnih zakonov, je sicer kar prosta grupa $F_2 = \langle x, y \rangle$. Če bi bila netrivialna beseda $w \in F_2 = \langle a, b \rangle$ zakon v njej, bi prišli do protislovja s preslikavo, ki jo inducirajo slike $x \mapsto a$, $y \mapsto b$.

5.2.1 Konstrukcija zakonov v grupah $PSL_2(q)$

Konstrukcija kratkih zakonov v grupah $\mathrm{PSL}_2(q)$ poteka prek obravnave redov elementov, praštevilskega izreka in uporabe komutatorske leme v slogu primera 3.7. Dokaz je prirejen po [17, str. 36–37] in [11].

Lema 5.9. *Red poljubnega element $A \in \mathrm{PSL}_2(q)$ deli vsaj eno izmed števil p, $q-1$ ali $q+1$.*

Dokaz. Naj bo matrika $A \in \mathrm{PSL}_2(q)$. Obravnavajmo primere glede na njeno Jordanovo formo J_A. Naj bo $\chi_A(X) \in \mathbb{F}_q[X]$ karakteristični polinom matrike A.

1. Če je A diagonalizabilna, je njena Jordanova forma oblike

$$J_A = \begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix},$$

kjer sta $\alpha, \beta \in \mathbb{F}_q^*$ (0 ne moreta biti, ker je matrika A obrnljiva). Ker je $(\mathbb{F}_q^*, \cdot)$ grupa moči $q-1$, velja $\alpha^{q-1} = \beta^{q-1} = 1_{\mathbb{F}_q}$ in od tod $J_A^{q-1} = I$ oziroma $A^{q-1} = I$.

2. Če je $\chi_A(X)$ razcepen v $\mathbb{F}_q[X]$, vendar matrika A ni diagonalizabilna, mora biti njena Jordanova forma oblike

$$J_A = \begin{bmatrix} 1_{\mathbb{F}_q} & \alpha \\ 0 & 1_{\mathbb{F}_q} \end{bmatrix} = I + N.$$

Diagonalna elementa morata namreč oba biti enaka $1_{\mathbb{F}_q}$ po razmisleku v definiciji 5.7. Ker velja $J_A^p = (I+N)^p = I^p + N^p = I$, red matrike A deli p.

3. Če $\chi_A(X)$ ni razcepen v $\mathbb{F}_q[X]$, je razpecen v $\mathbb{F}_{q^2}[X] = \mathbb{F}_q[X]/(\chi_A(X))$. Naj bo $\alpha \in \mathbb{F}_{q^2}$ neka ničla $\chi_A(X)$. Pokazati moramo, da je potem tudi α^q njegova ničla. Naj bo $\chi_A(X) = X^2 + bX + c$ za neka $b, c \in \mathbb{F}_q^*$. Potem iz enačbe $\alpha^2 + b\alpha + c = 0$ sledi

$$0 = (\alpha^q + b\alpha + c)^q = \alpha^{2q} + b^q\alpha^q + c^q \overset{\text{1. točka}}{=} \alpha^{2q} + b\alpha^q + c.$$

Tako lahko matriko A diagonaliziramo v kolobarju $M_2(\mathbb{F}_{q^2})$ v obliki

$$J_A = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^q \end{bmatrix}.$$

Ker velja $\det A = \det J_A = \alpha\alpha^q = 1$, red A deli število $q + 1$.

□

Za konkretno grupo $G = \mathrm{PSL}_2(q)$ definirajmo podmnožice

$$H_m := \{A \in \mathrm{PSL}_2(q) |\, A^m = I\}$$

za števila $m \in \{p, q-1, q+1\}$. Po razmisleku iz prejšnje leme te podmnožice tvorijo pokritje G. V luči primera 3.7 je zakon v grupi G beseda oblike

$$\begin{aligned} w &= [[ba^pb^{-1}, a^{q-1}], a^{q+1}] \\ &= ba^pb^{-1}a^{q-1}ba^{-p}b^{-1}\cancel{a^{1-q}}a^{q+1}\cancel{a^{q-1}}ba^pb^{-1}a^{1-q}ba^{-p}b^{-1}a^{-q-1} \\ &= ba^pb^{-1}a^{q-1}ba^{-p}b^{-1}a^{q+1}ba^pb^{-1}a^{1-q}ba^{-p}b^{-1}a^{-q-1} \end{aligned}$$

dolžine

$$l(w) = 4(2 + p + q) \leq 8(q + 1).$$

Pred uporabo komutatorske leme moramo navesti še dva rezultata.

Lema 5.10.

$$|\mathrm{PSL}_2(q)| = \begin{cases} (q^2-1)q; & p = 2, \\ \frac{1}{2}(q^2-1)q; & p \neq 2. \end{cases}$$

Dokaz. Grupa $\mathrm{GL}_2(q)$ ima $(q^2-1)(q^2-q)$ elementov. Če hočemo, da je matrika $A \in M_2(\mathbb{F}_q)$ obrnljiva, imamo namreč za prvi stolpec $q^2 - 1$ izbir, za drugega pa $q^2 - q$. Od tod sledi, da ima $\mathrm{SL}_2(q)$ natanko $(q^2-1)q$ elementov, saj je $|\mathbb{F}_q^*| = q - 1$. V primeru $p \neq 2$, nam kvocient po centru odbije še polovico elementov. □

Zdaj se lahko lotimo konstrukcije netrivialnega zakona za grupe oblike $\mathrm{PSL}_2(q)$, moči manjše ali enake naravnemu številu n. Z uporabo lem 5.10 in **??** vemo, da moramo moramo konstruirati zakone za vse grupe $\mathrm{PSL}_2(q)$, za katere je $q \leq \sqrt[3]{(1 + o(1))2n}$. Od tod dobimo besedo $w \in F_2$ dolžine

$$l(w) \leq 8\left(\frac{3\sqrt[3]{(1+o(1))2n}}{\log((1+o(1))2n))}\right)^2 \cdot 8\sqrt[3]{(1+o(1))2n} \leq 1152(1+o(1))\frac{n}{\log(n)^2},$$

ki je zakon v vseh grupah $\mathrm{PSL}_2(q)$ moči n ali manj.

6 Iskanje zakonov z računalnikom

Na roke dokazati, da je beseda zakon, je – z izjemo posebnih primerov – zoprno. Zato je zelo naravno pomisliti na uporabo računalnika. V tem poglavju sta opisana dva različna pristopa za iskanje oziroma razumevanje zakonov v končnih grupah. Programa se nahajata v repozitoriju diplomske naloge `https://github.com/MightyOwler/Diplomska-naloga/` v mapi `Program_za_racunsko_iskanje_zakonov`.

6.1 Iskanje zakonov v grupah $\mathrm{PSL}_2(p)$

Najprimitivnejši način iskanja zakonov v dani grupi G je kar po definiciji: Poiščemo vse besede grupe $F_2 = \langle a, b \rangle$ določene dolžine, nato pa jih izvrednotimo na vseh možnih parih. Za začetek me je zanimalo, koliko zakonov dolžine 17 ali manj premorejo grupe $\mathrm{PSL}_2(p)$. Za višje dolžine je bilo potrebno generirati nepraktično veliko besed. Pri tem se zavedamo, da grupe $\mathrm{PSL}_2(p)$ ne morejo imeti zakonov dolžine p ali manj po trditvi 5.8. Program sem spisal v jeziku C++, ki je v splošnem veliko hitrejši od GAP-a, opisuje ga spodnja psevdokoda.

Algoritem 1 Generiranje besed in parov elementov ter preverjanje zakonov v $\mathrm{PSL}_2(p)$

Vhod: Brez vhodnih parametrov.
Izhod: Seznam besed, ki so zakoni v $\mathrm{PSL}_2(p)$ za določena praštevila p.

Generiranje besed in parov elementov
for $k \leftarrow 1$ **to** 17 **do**
    generiraj vse okrajšane besede dolžine k
    shrani jih v datoteko
end for
for each p **in** $\{2, 3, 5, 7, 11, 13, 17\}$ **do**
    predstavi elemente grupe $\mathrm{PSL}_2(p)$ kot 2×2 matrike
    generiraj vse pare elementov grupe $\mathrm{PSL}_2(p)$
    pare shrani v datoteko
end for
Preverjanje zakonov
for each p **in** $\{2, 3, 5, 7, 11, 13, 17\}$ **do**
    for $k \leftarrow p$ **to** 17 **do**
        preberi pare grupe $\mathrm{PSL}_2(p)$ in besede dolžine k iz generiranih datotek
        na vsaki besedi evalviraj vse pare
        if rezultat vseh evalvacij besede je identična matrika **then**
            ta beseda je zakon
        end if
    end for
end for

Hitro se je izkazalo, da je tak pristop zelo neučinkovit. Problem je namreč v tem, da število besed dolžine k narašča eksponentno. Če brez škode za splošnost fiksiramo prvo črko, je to število enako 3^{k-1}, saj lahko v vsakem koraku dodamo natanko 3 črke, da ne pride do krajšanja. Tudi če bi obravnavali zgolj tako imenovane *komutatorske*

besede, ki vsebujejo enako število črk kot njihovih inverzov (število črk a je enako številu črk a^{-1}, podobno za b), njihovo število mnogo prehitro narašča, da bi lahko pokazali karkoli smiselnega.

V splošnem se sicer da oceniti, z najmanj kolikšno verjetnostjo je naključna beseda $w \in F_2$ zakon v grupi G. Oceniti moramo indeks grupe zakonov $K(G,2)$ v grupi F_2. S pomočjo posledice 2.11 v primeru $k = 2$ dobimo oceno

$$[F_2 : K(G,2)] \leq |G|^{|G|^2},$$

kar vsekakor ni ravno spodbudno. Pa vendar se v praksi izkaže, da ti indeksi dejansko so razmeroma visoki. Članek [6] nam ponuja konkretne vrednosti naslednjih indeksov.

$$\begin{aligned}
[F_2 : K(D_{10},2)] &= 2^2 \cdot 5^5 = 12500,\\
[F_2 : K(\mathrm{Sym}(3),2)] &= 2^2 \cdot 3^5 = 972,\\
[F_2 : K(\mathrm{Alt}(4),2)] &= 2^{10} \cdot 3^2 = 9216,\\
[F_2 : K(\mathrm{Alt}(5),2)] &= 2^{48} \cdot 3^{24} \cdot 5^{24} \approx 4.73 \cdot 10^{42}.
\end{aligned}$$

V splošnem ni veliko grup, za katere bi poznali točne vrednosti teh kvocientov [6, str. 1]. Podobnih rezultatov za grupe $\mathrm{PSL}_2(q)$ nisem našel. Ker so te grupe za $q > 3$ enostavne ([11]), si za njihovo obravnavo z ugotovitvami naslednjega razdelka ne moremo pomagati.

6.2 Iskanje zakonov v nilpotentnih grupah

Kot smo videli v prejšnjem razdelku, moramo do problema pristopiti bolj zvito. Delež zakonov med vsemi dvočrkovnimi besedami nam določa kvocient

$$F_2 \Big/ \bigcap_{\varphi \in \mathrm{Hom}(F_2,G)} \ker \varphi.$$

Ni težko videti, da je grupa $F_2^{\exp(G)} = \langle w^{\exp(G)} \,|\, w \in F_2 \rangle$ edinka v F_2. Za poljubne besede $w_i \in F_2, u \in F_2$ in celo število n namreč velja $(\prod_i w_i^n)^u = \prod_i (w_i^u)^n$, tudi v primeru $n = \exp(G)$. Ni težko razmisliti, da je vsaka beseda $w \in F_2^{\exp(G)}$ zakon v grupi G, torej $F_2^{\exp(G)} \subseteq K(G,2)$. Za vsak par $g, h \in G$ namreč velja

$$w(g,h) = \prod_{i=1}^{n} w_i(g,h)^{\exp(G)} = \prod_{i=1}^{n} g_i^{\exp(G)} = 1_G.$$

Po tretjem izreku o izomorfizmu zapišemo

$$F_2 \Big/ \bigcap_{\varphi \in \mathrm{Hom}(F_2,G)} \ker \varphi \cong \frac{F_2/F_2^{\exp(G)}}{\bigcap\limits_{\varphi \in \mathrm{Hom}(F_2/F_2^{\exp(G)},G)} \ker \varphi}.$$

Tu se pojavi nezanemarljiv problem: v splošnem nam nič ne zagotavlja končnosti kvocienta $B(2,\exp(G)) := F_2/{F_2}^{\exp(G)}$. Pravzaprav smo prišli do klasičnega Burnsidovega problema, ki sprašuje po končnosti kvocientov oblike $B(m,n) := F_m/F_m^n$. Po rezultatu Lysenoka leta 1996 recimo velja, da je grupa $B(2,n)$ neskončna za $n \geq 8000$ ([22, str. 2]). Da lahko vseeno nadaljujemo s podobnim razmislekom, se osredotočimo na nilpotentne grupe. Potrebovali bomo naslednjo lemo, idejo za dokaz najdemo v [19, str. 13–14].

Lema 6.1. *Naj bo H končno generirana nilpotentna grupa razreda d in naj ima končni eksponent. Potem je H končna.*

Dokaz. Za začetek pokažimo, da so grupe $\gamma_i(H)/\gamma_{i+1}(H)$ Abelove za vsa števila $i \geq 1$. To sledi iz preprostega sklepa

$$\gamma_{i+1}(H) = [\gamma_i(H), H] \supseteq [\gamma_i(H), \gamma_i(H)].$$

Nato dokažimo, da je vsaka končno generirana Abelova grupa končnega eksponenta končna. Naj bo $K = \langle k_1, \ldots, k_m \rangle$ grupa, ki ustreza tem zahtevam. Ker lahko zaradi komutativnosti vsak element $k \in K$ zapišemo v obliki

$$k = k_1^{n_1} \cdots k_m^{n_m}$$

za neka števila $0 \leq n_i < \exp(K)$, je K res končna. Tako smo razmislili, da so končne vse grupe $\gamma_i(H)/\gamma_{i+1}(H)$ za $i \geq 1$. Ker je H nilpotentnta razreda H in velja

$$[H : \gamma_2(H)][\gamma_2(H) : \gamma_3(H)] \cdots [\gamma_d(H) : \gamma_{d+1}(H)] < \infty,$$

sklepamo, da je H končna. □

Predpostavimo, da je grupa G nilpotentna razreda d. Podobno kot v dokazu **??** sklepamo, da so vse besede iz $\gamma_{d+1}(F_2)$ zakoni v grupi G. Ker velja $\gamma_{d+1}(G) = \{1_G\}$, bo za vsako besedo $w \in \gamma_{d+1}(F_2)$ in vsak par elementov $g, h \in G$ veljalo $w(g, h) = 1_G$. Tako imamo $\gamma_{d+1}(F_2) \subseteq K(G, 2)$. Ker je poljubni člen spodnje centralne vrste edinka v F_2, je edinka tudi grupa $\gamma_{d+1}(F_2)$. Produkt edink je edinka, zato je tudi $F_2^{\exp(G)}\gamma_{d+1}(F_2)$ edinka v F_2, in lahko tvorimo kvocient

$$F_2 \Big/ \bigcap_{\varphi \in \mathrm{Hom}(F_2, G)} \ker \varphi \cong \frac{F_2/F_2^{\exp(G)}\gamma_{d+1}(F_2)}{\bigcap\limits_{\varphi \in \mathrm{Hom}(F_2/F_2^{\exp(G)}\gamma_{d+1}(F_2), G)} \ker \varphi}.$$

S tem smo problem v primeru nilpotentnih grup poenostavili, saj nam za izračun zakonov ni več treba računati jeder vseh homomorfizmov $F_2 \to G$, temveč le še $F_2/F_2^{\exp(G)}\gamma_{d+1}(F_2) \to G$. To je precej bolj ugodno, saj je grupa $F_2/F_2^{\exp(G)}\gamma_{d+1}(F_2)$ nilpotentna razreda največ d zaradi sklepa $\gamma_{d+1}(F_2) \subseteq F_2^{\exp(G)}\gamma_{d+1}(F_2)$. Posledično je po lemi 6.1 končna. Računalniška konstrukcija tega kvocienta ni posebej zahtevna, saj GAP vsebuje paket za delo z nilpotentnimi grupami `nq` ([10]), s pomočjo katerega ga lahko izračunamo in preučujemo njegovo grupno strukturo. Na tak način sem izračunal indekse za vse nilpotentne grupe do vključno moči 63, za višje vrednosti je bila časovna zahtevnost prevelika. Program in rezultati so objavljeni na repozitoriju `https://github.com/MightyOwler/Diplomska-naloga`. Program opisuje naslednja psevdokoda.

Ta pristop do problema je mnogo boljši od pristopa v razdelku 5.2, saj je ne le bolj povezan s strukturo grup, temveč tudi omogoča boljši vpogled v splošno razumevanje zakonov. Z njegovo pomočjo je namreč lažje opaziti in posledično dokazati naslednje lastnosti zakonov. Začnimo s preprostimi.

Algoritem 2 Izračun vrednosti in struktur za nilpotentne grupe

Vhod: Spodnja in zgornja meja moči nilpotentnih grup, ki jih bomo preučevali.
Izhod: Rezultati izračunanih grupnih struktur in velikosti kvocientov.

1: seznam_nilpotentnih ← seznam nilpotentnih grup želenih moči
2: **for each** G **in** seznam_nilpotentnih **do**
3: $e \leftarrow \exp(G)$
4: $d \leftarrow$ razred nilpotentnosti grupe G
5: kvocient $\leftarrow F_2/F_2^e\gamma_{d+1}(F_2)$
6: zakoni $\leftarrow \bigcap_{\varphi \in \mathrm{Hom}(F_2/F_2^e\gamma_{d+1}(F_2),G)} \ker\varphi$
7: poračunamo strukturo in velikost kvocienta kvocient/zakoni
8: **end for**
9: izračunane rezultate shranimo v datoteko

Trditev 6.2. *Za vsako ciklično grupo C_n je*

$$F_2/K(C_n,2) \cong C_n \times C_n$$

in posledično sledi

$$[F_2 : K(C_n,2)] = n^2.$$

Z drugimi besedami, delež zakonov med vsemi besedami v cikličnih grupah je $1/n^2$.

Dokaz. Naj bo $F_2 = \langle a, b\rangle$. Najti moramo epimorfizem $F_2 \to C_n \times C_n$ z jedrom $K(C_n,2)$. Na tej točki se spomnimo preprostega sklepa, da velja $K(C_n,2) = K(C_n \times C_n, 2)$. Naj bo $\xi \in C_n$ generator te ciklične grupe. Definirajmo preslikavo $\varphi : F_2 \to C_n \times C_n$, inducirano s slikama elementov $a \mapsto (\xi, 1_{C_n})$ in $b \mapsto (1_{C_n}, \xi)$. Ta preslikava je očitno surjektivna, preveriti moramo še, da je $\ker\varphi = K(C_n,2)$. Najprej preverimo inkluzijo $\ker\varphi \subseteq K(C_n,2)$. Naj bo $w \in \ker\varphi \subseteq F_2$ okrajšana beseda oblike $w = a^{r_1}b^{s_1}\ldots a^{r_k}b^{s_k}$ za neka cela števila $r_1, s_1, \ldots, r_k, s_k$. To pomeni, da je

$$\varphi(w) = \varphi(a^{r_1})\varphi(b^{s_1})\ldots\varphi(a^{r_k})\varphi(b^{s_k}) = \left(\xi^{r_1+\ldots+r_k}, \xi^{s_1+\ldots+s_k}\right) = (1_{C_n}, 1_{C_n}).$$

Z drugimi besedami, vsoti $r_1 + \ldots + r_k$ in $s_1 + \ldots + s_k$ morata biti deljivi z n. Zato imamo za poljubna elementa $g, h \in C_n$

$$w(g,h) = g^{r_1+\ldots+r_k}h^{s_1+\ldots+s_k} = 1_{C_n},$$

torej je w zakon v C_n. Dokažimo še $\ker\varphi \supseteq K(C_n,2)$. Naj bo $w \in K(C_n,2)$ okrajšana beseda oblike $w = a^{r_1}b^{s_1}\ldots a^{r_k}b^{s_k}$ za neka cela števila $r_1, s_1, \ldots, r_k, s_k$. Potem velja

$$\varphi(w) = \varphi(a)^{r_1}\varphi(b)^{s_1}\ldots\varphi(a)^{r_k}\varphi(b)^{s_k} = w(\varphi(a),\varphi(b)) = (1_{C_n}, 1_{C_n}).$$

Zadnja enakost sledi iz dejstva, da je w zakon v grupi C_n in posledično v $C_n \times C_n$. □

Posledica 6.3. *Naj bo grupa G elementarno Abelova, torej $G = \prod_{i=1}^n C_{p^{k_i}}$. Potem velja $F_2/K(G,2) \cong C_{p^k} \times C_{p^k}$, kjer je $k = \max_{i=1,\ldots,n} k_i$.*

Dokaz. Beseda $w \in F_2$ je zakon v C_{p^k} natanko tedaj, ko je zakon v vsakem faktorju produkta $\prod_{i=1}^{n} C_{p^{k_i}}$. Implikacija v levo je zato očitna, implikacija v desno pa tudi, saj za vsak $i = 1, \ldots, n$ velja $C_{p^{k_i}} \leq C_{p^k}$, zakoni pa se prenašajo na podgrupe. □

Posledica 6.4. *Naj bo končna grupa G Abelova. Natančneje, naj bo v skladu s klasifikacijo končnih Abelovih grup oblike $G = \prod_{i=1}^{n} \prod_{j=1}^{n_i} C_{p_i}^{m_j}$, kjer so za vsak $i = 1, \ldots, n$ p_i paroma različna praštevila, števila $n_i, m_i \geq 1$, in vsak $j = 1, \ldots, n_i$ števila $k_{i,j} \geq 1$ paroma različna. Naj bodo $k_i = \max_{j=1,\ldots,n_i} k_{i,j}$. Potem velja $F_2/K(G,2) \cong C_e \times C_e$, kjer je $e = p_1^{k_1} \cdots p_n^{k_n} = \exp(G)$. Od tod sledi, da delež zakonov v Abelovih grupah znaša natanko $1/\exp(G)^2$.*

Dokaz. V luči prejšnje posledice je beseda $w \in F_2$ zakon v grupi C_e natanko tedaj, ko je zakon v grupi $\prod_{i=1}^{n} C_{p^{k_i}}$, ki je po klasifikaciji končnih Abelovih grup izomorfna C_e. Nato uporabimo trditev 6.2. □

Intuitivno je to še lažje videti z naslednjim neformalnim razmislekom. Naj bo podana beseda $w \in F_2 = \langle a, b \rangle$. Če hočemo preveriti, ali je zakon v Abelovi grupi G, se lahko pretvarjamo, da črke med seboj komutirajo. Tako w prevedemo na besedo oblike $w' = a^r b^s$, kjer r in s predstavljata vsoto eksponentov črk a oziroma b v besedi w. Beseda a^r je zakon v grupi G natanko tedaj, ko je $\exp(G)$ delitelj števila r. Zato je verjetnost, da bo w zakon po črki a enaka $1/\exp(G)$. Ker enako velja za b in sta evalvaciji a in b medsebojno neodvisni, je skupna verjetnost enaka $1/\exp(G)^2$.

6.3 Problemi za nadaljnje raziskovanje

Med preučevanjem zakonov z računalnikov sem naletel na nekaj problemov, ki jih nisem znal rešiti, predvsem v zvezi s semidirektnim produktom grup.

Definicija 6.5. Naj bo G grupa, $N \trianglelefteq G$ njena edinka in $H \leq G$ njena podgrupa. Naj bo $\varphi \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ homomorfizem. Potem definiramo *semidirektni produkt* kot grupo nad množico $N \times H$, z operacijo

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \varphi(h_1)(n_2), h_1 h_2).$$

Označimo jo z $N \rtimes_\varphi H$.

Opomba 6.6. Za različne izbire homomorfizma $\varphi \in \mathrm{Hom}(H, \mathrm{Aut}(N))$ dobimo grupe, ki med seboj niso nujno izomorfne. Poglejmo si denimo primera $C_n \rtimes_{\mathrm{id}} C_2$ in $C_n \rtimes_\tau C_2$, kjer sta $\mathrm{id}(h)(g) = g$ in $\tau(h)(g) = hgh^{-1}$ za vsaka elementa $h \in C_2$ in $g \in C_n$. Očitno velja $C_n \rtimes_{\mathrm{id}} C_2 = C_n \times C_2$. Manj očitno pa je

$$C_n \rtimes_\tau C_2 = D_{2n}.$$

To lahko preverimo prek veljavnosti enačb $(g, 1_H)^n = 1_{C_n \rtimes_\tau C_2}$, $(1_N, h)^2 = 1_{C_n \rtimes_\tau C_2}$ in $((g, 1_H)(1_N, h))^2 = (g, h)^2 = 1_{C_n \rtimes_\tau C_2}$ za vse elemente $g \in N$ in $h \in H$.

Ta opomba nam sporoča, da je tudi grupa zakonov semidirektnega produkta odvisna od izbire homomorfizma φ. Imamo namreč

$$C_3 \rtimes_{\mathrm{id}} C_2 = C_3 \times C_2 = C_6 \quad \text{in} \quad C_3 \rtimes_\tau C_2 = D_6 = \mathrm{Sym}(3).$$

Iz razdelka 6.2 vemo, da velja $[F_2 : K(C_6, 2)] = 36$ in $[F_2 : K(\mathrm{Sym}(3), 2)] = 972$, zato grupi $K(C_6, 2)$ in $K(\mathrm{Sym}(3), 2)$ nista izomorfni.

Domneva 6.7. Za vsako praštevilo p in naravno število $k > 1$ obstaja taka homomorfizma $\varphi, \psi \in \mathrm{Hom}(C_p, \mathrm{Aut}(C_{p^k}))$, da velja

$$F_2/K(C_{p^k} \rtimes_\varphi C_p, 2) = (C_{p^k} \times C_p) \rtimes_\psi C_{p^k}.$$

To domnevo sem empirično potrdil za $k = 2, 3, 4, 5$ pri praštevilu $p = 2$ in $k = 2$ pri $p = 3$. Poraja se tudi vprašanje, kakšne oblike morata biti homomorfizma φ in ψ.

Domneva 6.8. Definirajmo *posplošeno kvaternionsko grupo reda* $4n$ kot

$$Q_{4n} := \langle r, Z | r^{2n} = Z^4 = 1,\ Z^{-1}rZ = r^{-1} \rangle$$

in *kvazidiedrsko grupo reda* 2^n kot

$$QD_{2^n} := \langle r, Z | r^{2^{n-1}} = Z^2 = 1,\ ZrZ = r^{2^{n-2}-1} \rangle.$$

Za vsako število $k \geq 2$ so grupe zakonov $K(D_{2 \cdot 2^{k-1}}, 2)$, $K(Q_{4 \cdot 2^{k-2}}, 2)$ in $K(QD_{2^k}, 2)$ izomorfne.

Ta domneva izhaja iz empirično izračunanega dejstva, da za vsako grupo $G \in \{D_{16}, Q_{16}, QD_{16}\}$ lahko zapišemo

$$F_2/K(G, 2) \cong (C_2 \times ((C_4 \times C_2) \rtimes_{\varphi_{G,1}} C_8)) \rtimes_{\varphi_{G,2}} C_8$$

za ustrezna homomorfizma $\varphi_{G,1}$ in $\varphi_{G,2}$. Enako velja za $2 \leq k \leq 5$. Seveda nam ta zapis ne zagotavlja, da so kvocienti med seboj izomorfni, kot smo videli v opombi 6.6. Morda pa se bistvo skriva ravno v tem, da so homomorfizmi $\varphi_{G,i}$ za različne grupe različni, kar privede do neizomorfnosti kvocientov.

7 Zaključek

Tekom naloge smo videli, kako potekajo raznorazne konstrukcije kratkih zakonov, tako konstruktivne kot z uporabo naključnih sprehodov. Upam, da mi je uspelo jasno pokazati, zakaj nas zanimajo prav nilpotentne, rešljive, enostavne in simetrične grupe in kako se naravno pojavijo kot zaporedje osnovnih sklepov prek uporabe razširitvene in komutatorske leme.

Za konec predstavimo še nekaj vprašanj za nadaljnje raziskovanje.

- Ali se da natančno določiti grupe, v katerih obstajajo netrivialni zakoni? Tega problema se dotakne članek [16], ki pokaže, da zakoni obstajajo v vseh grupah, katerih rast glede na neko generatorsko podmnožico je polinomska. Po Gromovem izreku [9] so to namreč virtualno nilpotentne grupe, ki po razširitveni lemi imajo netrivialne zakone.
- Ali bi lahko uporabili naključne sprehode za analizo nilpotentnih oziroma rešljivih grup (in ali je to sploh smiselno)?
- Na katerih družinah grup bi lahko smiselno uproabili računalniško konstrukcijo iz zadnjega poglavja?
- Katere druge ugotovitve o deležu zakonov med besedami lahko dokažemo s pomočjo izračunanih kvocientov?
- Kako bi lahko naše znanje bolj tesno povezali z Burnsidovimi problemi?
- Ali bi lahko naše znanje uporabili za napad Amit–Ashurstine domneve (glej [5])?

Slovar strokovnih izrazov

group law/identity zakon v grupi
nilpotent group nilpotentna grupa
solvable group rešljiva grupa
simple group rešljiva grupa
non-trivial power periodični element
symmetric group simetrična grupa
lower central series spodnja centralna vrsta
derived series izpeljana vrsta
(lazy) random walk (leni) naključni sprehod

Literatura

[1] *Nilpotent group*, 2024, dostopno na https://en.wikipedia.org/wiki/Nilpotent_group, ogled: 18. 8. 2024.

[2] N. avtor, *Free groups are torsion-free*, https://math.stackexchange.com/questions/2207776/free-groups-are-torsion-free, 2017, [ogled 24. 8. 2024].

[3] N. avtor, *Injective map needed in definition of free groups*, https://math.stackexchange.com/questions/4689399/injective-map-needed-in-definition-of-free-groups, 2023, [ogled 24. 8. 2024].

[4] H. Bradford in A. Thom, *Short laws for finite groups and residual finiteness growth*, 2017, dostopno na https://arxiv.org/abs/1701.08121, verzija 1. 7. 2022 [ogled 29. 2. 2024].

[5] B. S. Chibelius, W. Cocke in M.-C. Ho, *Enumerating word maps in finite groups*, International Journal of Group Theory **13**(3) (2016) 307–318.

[6] W. Cocke in D. Skabelund, *The free spectrum of a5*, International Journal of Algebra and Computation **30**(04) (2020) 685–691, dostopno na https://doi.org/10.1142/S0218196720500162.

[7] A. Elkasapy in A. Thom, *On the length of the shortest non-trivial element in the derived and the lower central series*, 2013, dostopno na https://arxiv.org/abs/1311.0138, verzija 1. 10. 2013 [ogled 29. 2. 2024].

[8] A. Granville, *Herald cramer and the distribution of prime numbers*, 1993, dostopno na https://web.archive.org/web/20150923212842/http://www.dartmouth.edu/~chance/chance_news/for_chance_news/Riemann/cramer.pdf.

[9] M. Gromov, *Groups of polynomial growth and expanding maps*, Institut des Hautes Études Scientifiques. Publications Mathématiques (53) (1981) 53–73.

[10] M. Horn in W. Nickel, *nq, nilpotent quotients of finitely presented groups, Version 2.5.11*, https://gap-packages.github.io/nq/, 2024, refereed GAP package.

[11] U. Jezernik, *Teorija upodobitev*, 2023, dostopno na https://urbanjezernik.github.io/teorija-upodobitev/, ogled: 18. 8. 2024.

[12] G. Kozma in A. Thom, *Divisibility and laws in finite simple groups*, Mathematische Annalen **364**(1-2) (2016) 79–95.

[13] R. Lyndon in P. Schupp, *Combinatorial group theory*, Springer Science and Business Media, 2015.

[14] MIT, *Lecture notes for 18.785, fall 2021*, https://math.mit.edu/classes/18.785/2021fa/LectureNotes16.pdf, 2021, [ogled 24. 8. 2024].

[15] B. Riemann, *Ueber die anzahl der primzahlen unter einer gegebenen grösse*, Monatsberichte der Berliner Akademie (1859), dostopno na https://www.claymath.org/wp-content/uploads/2023/04/Wilkins-transcription.pdf.

[16] S. Schleimer, *On the girth of groups* (2001).

[17] J. Schneider, *On the length of group laws*, magistrsko delo, Technische Universität Dresden, Department of mathematics, 2016.

[18] M.-P. Schützenberger, *Sur l'équation* $a^{2+n} = b^{2+m}c^{2+p}$ *dans un groupe libre*, Comptes rendus de l'Académie des Sciences Paris, Série I Mathématique **248** (1959) 2435–2436, dostopno na https://www-igm.univ-mlv.fr/~berstel/Mps/Travaux/A/1959EquationGroupeLibreCRAS.pdf.

[19] D. Segal, *Polycyclic Groups*, Cambridge Tracts in Mathematics, Cambridge University Press, 1983.

[20] J. P. Souvent, *Proste grupe in drevesa*, Matrika **11**(1) (2024), dostopno na https://matrika.fmf.uni-lj.si/letnik-11/stevilka-1/pogacnik.pdf.

[21] A. Thom, *About the length of laws for finite groups*, 2015, dostopno na https://arxiv.org/abs/1508.07730, verzija 5. 9. 2015 [ogled 29. 2. 2024].

[22] M. Vaughan-Lee in E. I. Zel'manov, *Bounds in the restricted burnside problem*, Journal of the Australian Mathematical Society **67**(2) (1999) 261–271, doi: 10.1017/S144678870000121X.

[23] A. Wikipedije, *List of finite simple groups — wikipedia, the free encyclopedia*, 2024, dostopno na https://en.wikipedia.org/wiki/List_of_finite_simple_groups, [ogled 24. 8. 2024].

[24] U. Wikipedije, *Cayley graph — wikipedia, the free encyclopedia*, https://en.wikipedia.org/wiki/Cayley_graph#/media/File:Cayley_graph_of_F2.svg, 2024, ogled: 18. 8. 2024.