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

TODO

Short Group Laws

ABSTRACT

TODO

Math. Subj. Class. (2020): 20, 05C81
Ključne besede: ..., ...
Keywords: ..., ...

1 Uvod

Dvočrkovni zakon v grupi G je abstrakten produkt elementov x, y ter njunih inverzov x^{-1} in y^{-1}, ki ima lastnost, da za vsako zamenjavo x in y s konkretnima elementoma $g, h \in G$ dobimo rezultat $1 \in G$.

Opomba 1.1. Definicijo n-črkovnih zakonov dobimo tako, da v zgornji definiciji elementa x, y (in njuna inverza) nadomestimo z elementi $x_1, x_2, \ldots, x_n$ (in njihovimi inverzi), ki jih zamenjujemo s konkretnimi elementi $g_1, g_2, \ldots, g_n \in G$.

Zakonu 1 pravimo trivialni zakon, ki v kontekstu raziskovanja zakonov ni posebej zanimiv. Najosnovnejši primer netrivialnega zakona se pojavi pri Abelovih grupah, kjer za poljubna elementa $x, y \in G$ velja $xy = yx$, kar je ekvivalentno zahtevi

$$xyx^{-1}y^{-1} = [x, y] = 1.$$

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

2 Osnovni pojmi

Definicijo zakona **??** lahko bolj formalno zapišemo s pomočjo prostih grup.

Definicija 2.1. Naj bo S množica. Grupa $F(S)$ je (do izomorfizma natančno) enolična grupa z lastnostjo, da za poljubno grupo G in poljubno preslikavo $\varphi : S \to G$ obstaja natanko ena razširitev $\varphi : F(S) \to G$, ki je hkrati homomorfizem grup.

Opomba 2.2. Za poljubni množici S in T velja $F(S) \cong F(T)$ natanko tedaj, ko $|S| = |T|$. Zato lahko v primeru končne množice $|S| = k$ govorimo o prosti grupi ranga k, ki jo označimo z F_k.

V viru ([5, str. 4, tridtev 1.9]) je natančno razloženo znano dejstvo, da lahko elemente proste grupe $F(S)$ predstavimo v obliki okrajšanih besed, torej besed oblike $w = s_1 \cdots s_n$, kjer je $s_i \in S \cup S^{-1}$ za $i = 1, \ldots, n$ in $s_i \neq s_{i+1}^{-1}$ za $i = 1, \ldots, n-1$. Tu je $S^{-1} = \{s^{-1} | \, s \in S\}$. Z upoštevanjem tega dejstva lahko elementom proste grupe $F(S)$ določimo dolžino.

Definicija 2.3. Naj bo $w \in F(S)$ element proste grupe nad množico S in naj bo njegova okrajšana oblika $w = s_1 \cdots s_n$. Potem številu n pravimo dolžina (besede) w in pišemo $l(w) = n$.

Zdaj definiramo izginjajočo množico besede w v grupi G.

Definicija 2.4. Naj bo $w \in F_k$. Potem množico

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

imenujemo izginajoča množica besede w v grupi G. Tu 1 označuje enoto v grupi G, $w(g_1, \ldots, g_k)$ pa sliko elementa $w \in F_k = \langle a_1, \ldots, a_k \rangle$ s homomorfizmom, induciranim s preslikavo $\varphi : a_i \mapsto g_i$ za $i = 1, \ldots, n$ v skladu z definicijo 2.1.

Zdaj lahko natančno formuliramo definicjo zakona.

Definicija 2.5. Beseda $w \in F_k$ je k-črkovni zakon v grupi G, če je $Z(G, w) = G^k$. Alternativno, beseda $w \in F_k$ je k-črkovni zakon v grupi G, če jo vsak homomorfizem $\varphi : F_k \to G$ slika v enoto $1 \in G$.

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

$$K(k) = \bigcap_{\varphi : F_k \to G} \ker(\varphi).$$

Ta množica je končni presek edink v G in posledično tudi sama edinka. Še več, invariantna je za vsak avtomorfizem $\alpha : F_k \to F_k$, saj

$$K(k) = \bigcap_{\varphi : F_k \to G} \ker(\varphi) = \bigcap_{\varphi : F_k \to G} \ker(\varphi \circ \alpha).$$

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

Lema 2.6. *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 $S := H_1 \cup H_2$. Naj bosta C_1 in C_2 množici odsekov podgrup H_1 in H_2 v G ter naj bo C množica odsekov podgrupe S v G. Definiramo preslikavo $f : C \to C_1 \times C_2$ s predpisom $f(gS) = (gH_1, gH_2)$. Desna smer sklepa

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

nam podaja dobro definiranost, leva pa injektivnost preslikave f, ki nam da $|C| \leq |C_1||C_2|$. $\square$

Z uporabo te leme direktno sledi, da je grupa $K(k)$ podgrupa končnega indeksa v F_k. To dejstvo bo še posebej pobmembno pri iskanju zakonov z računalnikom.

Definicija 2.7. Število

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

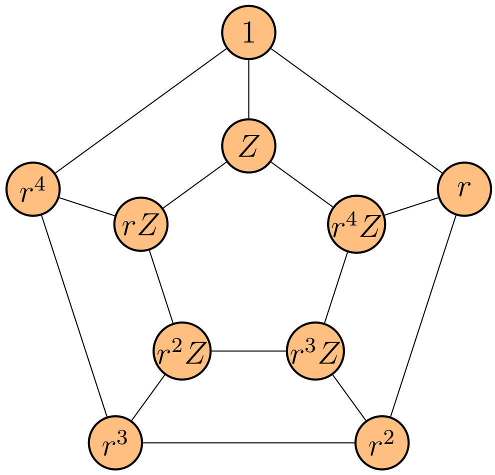
je k-črkovna dolžina grupe G.

Definicija 2.8. Naj bo G grupa in $S \subseteq G$ njena podmnožica, za katero velja $S = S^{-1}$. 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 2.9. Pogoj simetričnosti $S = S^{-1}$ nam pove, da je $\mathrm{Cay}(G, S)$ pravi graf in ne zgolj usmerjen. Imamo namreč

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

Primer 2.10. Na spodnjih slikah imamo Cayleyjev graf grupe diedrske grupe $D_{10} = \langle r, Z \rangle$ za različni generatorski množici. TODO nariši desno od tega še graf s 5 generatorji, morda raje Cayleyjev graf proste grupe F2, saj nastopa naslednji trditvi



$\diamondsuit$

Opomba 2.11. Ime ožina je smiselno v kontekstu definicije Cayleyjevega grafa grupe. TODO zakaj

Izkaže se, da so najbolj zanimivi in za obravnavo relevantni dvočrkovni zakoni. To nam sporočata naslednji dve trditvi.

Trditev 2.12. *Obstaja vložitev grupe $F_{2\cdot 3^k} = \langle x_1, \ldots, x_{2\cdot 3^k} \rangle$ v grupo $F_2 = \langle x, y \rangle$, da velja $l(x_i) = 2k + 1$, kjer $l(w)$ označuje dolžino besede $w \in F_2 = \langle x, y \rangle$.*

Dokaz. Dokaz trditve je nekoliko preveč tehničen za potrebe te naloge, naveden v [6]. Glavna ideja je, da obravnavamo Cayleyev graf proste grupe F_2 z dvema generatorjema. Drevo vseh besed dolžine k na ustrezen način dopolnimo tako, da dodamo povezave listom. Pri tem dobimo cikle dolžine $2k + 1$ in utemeljimo, da lahko jih lahko obravnavamo kot elemente $F_{2\cdot 3^k}$, vložene v F_2. $\square$

Posledica 2.13. *Naj bo G grupa in $k \geq 2$ naravno število. Potem velja*

$$\mathrm{girth}_k(G) \leq \mathrm{girth}\, 2(G)$$

in

$$\mathrm{girth}_2(G) \leq \left(2 \left\lceil \log_3(\frac{k}{2}) \right\rceil + 1\right) \mathrm{girth}_k(G).$$

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

3 Komutatorska in razširitvena lema

3.1 Komutatorska lema

Recimo da nekatere že poznamo zakone za grupe oziroma njihove podmnožice, zanima pa nas, kako bi iz njih zgradili nove zakone. Na to vprašanje odgovarjata komutatorska in razširitvena lema, ki sta ključni orodji pri obravnavanju zakonov. Preden ju dokažemo moramo pokazati nekaj rezultatov.

Definicija 3.1. Naj bo G grupa. Element $g \in G$ je netrivialna potenca, če obstajata $h \in G$ in naravno število $n > 1$, da je $g = h^n$.

Lema 3.2 ([5][str. 8, trditev 2.6)**.** *] Vsaka končnogenerirana podgrupa proste grupe je prosta.*

Ta lema je posebni primer klasičnega Nielsen–Schreierjevega izreka, ki pravi, da je vsaka podgrupa proste grupe prosta. Dokazana je v [5][5–7] z uporabo Nielsenovih transformacij.

Lema 3.3. *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 beseda $w \in F_k$ dolžine*

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

ki ni netrivialna potenca, da za vsako grupo G velja

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

Dokaz. Dokaz poteka z indukcijo po $e \in \mathbb{N}$. Naj bo $F_k = \langle S \rangle$. Za $e = 0$ (oziroma $m = 1$) vzamemo $w = [s, w_1]$, kjer je $s \in S$ takšen element, da w_1 ni potenca s. To lahko storimo zaradi pogoja $k \geq 2$. Zaradi ustrezne izbire komutator $[s, w_1]$ ne more biti netrivialna potenca, njegova dolžina pa je kvečjem $2(l(w_1) + 1)$. Hkrati 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 besedi $v_1, v_2 \in F_k$, ki nista netrivialni potenci, da velja

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

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

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 utemeljiti, da lahko besedi v_1 ter v_2 ustrezno združimo. Vemo, da je komutator $[a, b]$ za $a, b \in F_k \setminus \{1\}$ trivialen natanko tedaj, ko a in b generirata prosto grupo ranga 1. Po lemi 3.2 namreč vemo, da je podgrupa $\langle a, b\rangle \leq F_k$ prosta, hkrati pa a in b po pogoju komutirata. Implikacija v levo je očitna. Zato vemo, da bo komutator $[v_1, v_2]$ trivialen zgolj v primeru $v_1 = v_2^{\pm 1}$, ker sta v_1 in v_2 po predpostavki netrivialni potenci. V primeru, da sta trivialni, imamo

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

in lahko nastavimo $w := v_1$ ali $w := v_2$, v obeh primerih je pogoj na dolžino besede w očitno izpolnjen. Če imamo $v_1 \neq v_2^{\pm 1}$, nastavimo $w := [v_1, v_2]$. V tem primeru po (TODO Schutzenbergovi lemi) beseda w ni netrivialna potenca.Indukcijska predpostavka nam zagotavlja

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

□

To lemo lahko posplošimo tako, da velja tudi za števila besed, ki niso dvojiške potence.

Lema 3.4. *Naj bo $k \geq 2$ in naj bodo podane netrivialne besede $w_1, \ldots, w_m \in F_m$. Potem obstaja beseda $w \in F_k$ dolžine*

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

ki ni netrivialna potenca, 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 2^e najmanjša dvojiška potenca, večja ali enaka m. Potem velja $2^e < 2m$ in nastavimo

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

□

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

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

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

Dokaz. To je direktna posledica leme 3.4 skupaj z dejstvom, da je

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

□

3.2 Razširitvena lema

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

Definicija 3.6. 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 $\ker\psi = \operatorname{im}\varphi$, φ je injektivni in ψ surjektivni homomorfizem.

Lema 3.7. *Naj bo*

$$\mathbf{1} \to N \to G \to G/N \to \mathbf{1}$$

kratko eksaktno zaporedje grup. Naj bo $F_k = \langle x_1, \ldots, x_k \rangle = \langle S \rangle$. Naj bo $w_N \in F_k$ netrivialni zakon za N in $w_G N \,/\!\!\in F_k$ netrivialni zakon za G/N. Potem obstaja netrivialni k-črkovni zakon za grupo G dolžine kvečjem $l(w_N)l(w_{G/N})$. Od tod sledi

$$\operatorname{girth}_k(G) \le \operatorname{girth}_k(N) \operatorname{girth}_k(G/N).$$

Dokaz. Dokaz obravnava dva možna primera oblike zakona za $w_{G/N}$.

1. Če je $w_{G/N} = s^n$ za neki $s \in S$, $n \in \mathbb{Z} \setminus \{0\}$, so vse besede oblike t^n, kjer je $t \in S$, zakoni za G/N. Zato lahko vzamemo besedo

   $$w = w_N(x_1^n, \ldots, x_k^n),$$

   ki je netrivialni zakon za G. To sledi iz dejstev, da preslikava $g \mapsto g^n$ slika G v N (ker je s^n zakon za G/N), w_N pa je netrivialni zakon za N.

2. Sicer lahko brez škode za splošnost predpostavimo, da je zakon oblike $w_{G/N} = x_1 w'_{G/N} x_2$, kjer se $w'_{G/N}$ niti ne začne z x_1^{-1} niti konča z x_2^{-1}. To smemo storiti, ker lahko na besedi uporabimo ciklino rotacijo in vzamemo $w''_{G/N} = sw't$, pri čemer $s, t \in S \cup S^{-1}$ in $st \neq 1$. Če je potrebno, lahko na tej besedi uporabimo avtomorfizem grupe F_k, ki ga inducirajo $s \mapsto x_1$, $x_1 \to s$, $x_2 \mapsto t$, $t \mapsto x_2$ in $r \mapsto r$ za vse ostale $r \in S$. Nato definiramo besede

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

   Ni težko preveriti, da so netrivialne kombinacije 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 $i, j \in \{1, \ldots, k\}$, $i \neq j$, v okrajšani obliki. Zato je

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

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

□

4 Nilpotentne in rešljive grupe

Definicija 4.1. 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 4.2. 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 katero je $G^{(d)} = \mathbf{1}$ rečemo razred rešljivosti grupe G.

Celo družino primerov nilpotentnih grup nam podaja naslednja ugotovitev.

Trditev 4.3. *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. TODO, tole ne bi smelo biti težko, samo moraš paziti, da je v skladu s spodnjo centralno vrsto. □

Primer 4.4. Trditev 4.3 nam sporoča, da so vse diedrske grupe oblike $D_{2\cdot 2^k}$ nilpotentne. Izkaže se, da so to tudi vse, saj (TODO tukaj moraš končati razmislek z dokazom https://math.stackexchange.com/questions/834966/is-the-dihedral-group-d-n-nilpotent-solvable). ♢

Definicija 4.5. 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 katero je $G^{(d)} = \mathbf{1}$ rečemo razred rešljivosti grupe G.

Primer 4.6. Diedrske grupe D_2n so rešljive razreda 2, saj imamo zaporedje (TOOD dokaži, kako izgleda to zaporedje.). ♢

Primer 4.7. Vse nilpotentne grupe so rešljive, saj po definiciji za vsako število $k \geq 0$ velja

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

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

Za rešljive grupe veljajo naslednje osnovne lasnosti.

Trditev 4.8.

1. *Vsaka podgrupa rešljive grupe je rešljiva.*
2. *Vsak kvocient rešljive grupe je rešljiv.*
3. *Naj bo $N \lhd G$ 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 $M, N \lhd G$ rešljivi razreda d_M oziroma d_N. Potem je podgrupa 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 $N \lhd G$. 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 $n_{G/N}$, 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 $k \geq d_M + d_N$.

4. Dokaz je povzet po opombi 4 iz [6, 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, sta po drugi točki trditve tudi grupi $N/(N \cap M)$ in MN/M rešljivi razreda d_N. 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 nam ponuja naslednjo skromno oceno dolžine kratkih netrivialnih zakonov v rešljivih oziroma nilpotentnih grupah.

Trditev 4.9. *Obstaja beseda $w \in F_2$ dolžine $l(w) \leq 4^d$, ki je zakon v vseh grupah razreda rešljivosti (ali nilpotentnosti) d ali manj.*

Dokaz. Tritev je posledica razširitvene leme 3.7, dokaz poteka z indukcijo po d. Za $d = 1$ je grupa G Abelova, zato je ustrezni zakon beseda $w = [x, y]$, 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 za grupo G. Za nilpotentne grupe upoštevamo dejstvo $G^{(1)} \subseteq \gamma_1(G)$, kar implicira komutativnost grupe $G/\gamma_1(G)$. □

Opomba 4.10. V članku [4, str. 8] je podana nekoliko šibkejša meja $l(w) \leq 4 \cdot 6^{d-1}$, ker je avtor uporabil šibkejšo obliko razširitvene leme.

4.1 Konstrukcija kratkih zakonov za nilpotentne in rešljive grupe

Konstrukcija kratkih zakonov za nilpotentne grupe je opisana v članku [3] in z razlagami dopolnjena v magistrskem delu [6]. Glavna ideja je, da poiščemo kratke netrivialne besede, vsebovane v izpeljani vrsti proste grupe $F_2 = \langle a, b \rangle$. Najprej definiramo zaporedji $(a_n)_n$ in $(b_n)_n$ v F_2 s predpisoma

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

Besede, ki jih bomo konstruirali s tema zaporedjema, morajo biti netrivialne, zato potrebujemo naslednjo lemo (lema 3.1 v viru [4] oziroma lema 8 v [6]).

Lema 4.11. *Za vsak $n \in \mathbb{N}$ so besede $a_n a_n$, $a_n^{-1} a_n^{-1}$, $b_n b_n$, $b_n^{-1} b_n^{-1}$, $a_n^{-1} b_n$, $b_n^{-1} a_n$, $a_n b_n^{-1}$, $b_n a_n^{-1}$, $a_n^{-1} b_n^{-1}$ in $b_n a_n$ v okrajšani obliki.*

Dokaz. Dokaz poteka z indukcijo po n. Za $n = 0$ je tridtev očitna, ker sta a in b različna generatorja grupe F_2. Za $n > 0$ razpišimo produkt $a_n a_n$.

$$a_n a_n = [b_{n-1}^{-1}, a_{n-1}]^2 = b_{n-1}^{-1} a_{n-1} b_{n-1} \underbrace{a_{n-1}^{-1} b_{n-1}^{-1}}_{\text{ni krajšanja}} a_{n-1} b_{n-1} a_{n-1}^{-1}$$

Ker po indukcijski predpostavki vemo, da ne more priti do krajšanja v produktu $a_{n-1}^{-1} b_{n-1}^{-1}$, ne more priti do krajšanja v produktu $a_n a_n$ ali njegovem inverzu $a_n^{-1} a_n^{-1}$. Enako sklepamo za preostale produkte.

- Produkt $b_n b_n$ in njegov inverz sta okrajšana, ker je okrajšan $b_{n-1}^{-1} a_{n-1}$.
- Produkt $a_n^{-1} b_n$ in njegov inverz sta okrajšana, ker je okrajšan $b_{n-1} a_{n-1}$.
- Produkt $b_n b_n^{-1}$ in njegov inverz sta okrajšana, ker je okrajšan $a_{n-1}^{-1} b_{n-1}$.
- Produkt $a_n^{-1} b_n^{-1}$ in njegov inverz sta okrajšana, ker je okrajšan $b_{n-1} b_{n-1}$.

□

Opomba 4.12. Produkti oblike $a_n b_n$ oziroma njihovi inverzi $b_n^{-1} a_n^{-1}$ niso nujno okrajšane besede, na primer že za $n = 1$ dobimo $a_1 b_1 = b^{-1} a b a a^{-1} b a^{-1} b^{-1}$. To dejstvo bomo izkoristili v nadaljevanju.

Najprej se prepričajmo, da so besede a_n oziroma b_n res elementi izpeljane grupe $F_2^{(n)}$.

Lema 4.13.

Dokaz. Dokaz poteka z indukcijo po n. Za $n = 0$ je očitno $a_0 = a \in F_2 = F_2^{(0)}$ in $b_0 = b \in F_2 = F_2^{(0)}$. Za $n > 0$ velja $a_{n+1} = [b_n^{-1}, a_n] \in \left[F_2^{(n)}, F_2^{(n)}\right] = F_2^{(n+1)}$ in $b_{n+1} = [a_n, b_n] \in \left[F_2^{(n)}, F_2^{(n)}\right] = F_2^{(n+1)}$. □

Nato ocenimo dolžino členov zaporedij $(a_n)_n$ in $(b_n)_n$.

Lema 4.14. *Za vsak $n \in \mathbb{N} \cup \{0\}$ velja $4^n \geq l(a_n) = l(b_n) \geq 2^n$.*

Dokaz. Po definiciji zaporedja $(b_n)_n$ velja

$$\begin{aligned} l(b_{n+1}) &= l(a_n b_n a_n^{-1} b_n^{-1}) \\ &= l(a_n b_n) + l(a_n) + l(b_n) \\ &= l(b_n^{-1} a_n b_n a_n^{-1}) \\ &= l(a_{n+1}) \end{aligned}$$

Za sklep v drugi in tretji vrstici je bila potrebna lema 4.11 ter preprost sklep, da za besedi $w_1, w_2 \in F_2$, za kateri je produkt $w_1 w_2$ okrajšan, velja $l(w_1 w_2) = l(w_1) + l(w_2)$. Iz druge vrstice sledi $l(b_{n+1}) \geq 2l(b_n)$ od koder z indukcijo dobimo $l(a_n) = l(b_n) \geq 2^n$. Iz tretje vrstice dobimo $l(b_{n+1}) \leq 4l(b_n)$ od koder z indukcijo sledi $l(b_n) \leq 4^n$, kar zopet dokaže oceno 4.16. □

Vrednost splošnega člena zaporedja $c_n := l(a_n) = l(b_n)$ nam podaja dolžino netrivialne besede v grupi $F_2^{(n)}$.

Lema 4.15. *Zaporedje $(c_n)_n$ ustreza rekurzivni zvezi $c_{n+2} = 3c_{n+1} + 2c_n$ z začetnima členoma $c_0 = 1$ in $c_1 = 4$. Od tod lahko izrazimo*

$$c_n = \left(\frac{1}{2} + \frac{5}{2\sqrt{17}}\right)\left(\frac{3+\sqrt{17}}{2}\right)^n + \left(\frac{1}{2} - \frac{5}{2\sqrt{17}}\right)\left(\frac{3-\sqrt{17}}{2}\right)^n \leq C_1\iota^n + o(1),$$

kjer je $\iota := (3+\sqrt{17})/2 = 3{,}5615528\ldots$ in $C_1 = 1/2 + 5/(2\sqrt{17})$.

Dokaz. Dokaz je v isti obliki podan v [6] in uporablja lemo 4.11.

$$\begin{aligned}
c_{n+2} &= l(b_{n+2}) \\
&= l([a_{n+1}, b_{n+1}]) \\
&= l([[b_n^{-1}, a_n], [a_n, b_n]]) \\
&= l(b_n^{-1}a_nb_n \underbrace{a_n^{-1}a_n}_{\text{se pokrajša}} b_na_n^{-1}b_n^{-1}) + l([a_n, b_n^{-1}]) + l([b_n, a_n]) \\
&= \underbrace{l(b_n^{-1}a_nb_n)}_{l(a_{n+1})-l(a_n^{-1})=c_{n+1}-c_n} + \underbrace{l(b_n) + l(a_n^{-1}) + l(b_n^{-1})}_{3c_n} + \underbrace{l([a_n, b_n^{-1}])}_{l(a_{n+1})=c_{n+1}} + \underbrace{l([b_n, a_n])}_{l(b_{n+1})=c_{n+1}}.
\end{aligned}$$

To nam da za $n \in \mathbb{N} \cup \{0\}$ želeno zvezo $c_{n+2} = 3c_{n+1} + 2c_n$ skupaj z začetnima vrednostima $c_0 = 1$ in $c_1 = 4$, kar nam podaja zvezo

$$\begin{bmatrix} c_{n+1} \\ c_n \end{bmatrix} = \underbrace{\begin{bmatrix} 3 & 2 \\ 1 & 0 \end{bmatrix}}_{A}^n \begin{bmatrix} 4 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{3-\sqrt{17}}{2} & \frac{3+\sqrt{17}}{2} \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \frac{3-\sqrt{17}}{2} & 0 \\ 0 & \frac{3+\sqrt{17}}{2} \end{bmatrix}^n \begin{bmatrix} -\frac{1}{\sqrt{17}} & \frac{1}{2} + \frac{3}{2\sqrt{17}} \\ \frac{1}{\sqrt{17}} & \frac{1}{2} - \frac{3}{2\sqrt{17}} \end{bmatrix} \begin{bmatrix} 4 \\ 1 \end{bmatrix}.$$

Z diagonalizacijo matrike A lahko iz druge vrstice razberemo zvezo iz trditve. Neenakost je posledica dejstva, da je po absolutni vrednosti največja lastna vrednost matrike A enaka $\iota = (3+\sqrt{17})/2 = 3{,}5615528\ldots$, kar je asimptotsko gledano veliko boljši rezultat od trditve 4.9. □

Direktna posledica te leme je naslednja ugotovitev za rešljive grupe.

Trditev 4.16. *Obstaja netrivialna besede $w \in F_2$, ki je zakon za vse grupe rešljivostnega razreda n ali manj, dolžine*

$$l(w) \leq C_1\iota^n + o(1),$$

kjer sta konstanti C_1 in ι enaki kot v lemi 4.15.

Dokaz. Naj bo G rešljiva grupa razreda k. Za poljubno besedo $w \in F_2^{(n)}$ za vsaka $g, h \in G$ velja – v skladu z oznakami iz definicije 2.4 – $w(g, h) \in G^{(n)}$. Ker je grupa G rešljiva razreda $k \leq n$, je $G^{(n)} = G^{(k)} = \{1_G\}$, torej bo w zakon za grupo G. Po prejšnji lemi obstaja netrivialna beseda dolžine $C_1\iota^n + o(1)$ v $F_2^{(n)}$, ki je iskani netrivialni zakon za grupo G. □

Zdaj moramo to znanje le še prevesti na nilpotentne grupe. Brez dokaza (najdemo ga lahko v TODO, ideja je ...) bomo privzeli naslednjo lemo.

Lema 4.17. *Za vsak $n \in \mathbb{N} \cup \{0\}$ velja inkluzija*

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

Naslednja trditev je kombinacija posledice 4 in leme 11 iz vira [6].

Trditev 4.18. *Obstaja netrivialna beseda $w \in F_2$, ki je zakon za vse nilpotentne grupe G moči največ n, dolžine*

$$l(w) \leq C_3 \log(n)^\kappa + o(1),$$

kjer sta $C_3 = 7{,}712869694\ldots$ in $\kappa = \log_2(\iota) = 1{,}832506\ldots$ konstanti.

Dokaz. Za vsako število $k \in \mathbb{N}$ je število $e = \lceil \log_2(k) \rceil$ najmanjše naravno število, da velja $k \leq 2^e \leq 2k$. Od tod po lemi 4.17 sledi

$$F_2^{(e)} \subseteq \gamma_{2^e}(F_2) \subseteq \gamma_k(F_2).$$

Po trditvi 4.16 obstaja netrivialna beseda $w \in F_2^{(e)}$ dolžine največ $C_1\iota^e + o(1)$. Zaradi izbira števila e lahko zapišemo

$$l(w) \leq C_1\iota^e = C_1 2^{\log_2(\iota)e} \leq C_1(2k)^{\log_2(\iota)} = C_1 \iota k^{\log_2(\iota)} = C_2 k^\kappa.$$

Nadalje naj bo grupa G nilpotentna razreda d, moči n ali manj. Zaradi nilpotentnosti G iz netrivialnosti grupe $\gamma_i(G)$ (za $i \in \mathbb{N} \cup \{0\}$) sledi netrivialnost kvocienta $\gamma_i(G)/\gamma_{i+1}(G)$, saj je centralna vrsta pred iztekom strogo padajoča. Za razred nilpotentnosti d velja ocena (TODO najdi vir) $d \leq \lfloor \log_2(G) \rfloor \leq \log_2(n)$. Zato po prvem sklepu dokaza obstaja netrivialna beseda $w \in \gamma_d(G)$ dolžine

$$l(w) \leq C_2 d^\kappa \leq C_2 \log_2(n)^\kappa = \frac{C_2}{\log_2(n)^\kappa} \log(n)^\kappa = C_3 \log(n)^\kappa,$$

saj velja $w \in \gamma_{\lfloor \log_2(n) \rfloor}(F_2) \subseteq \gamma_d(F_2)$. Od tod z analognim razmislekom kot v trditvi 4.16 sledi, da je w netrivialni zakon za vse nilpotentne grupe razreda d. $\square$

V nadaljevanju članka [3] avtorja eksponent κ iz prejšnje trditve izboljšata na $\lambda := 1{,}44115577\ldots$, pri čemer je treba namesto konstante C_3 vzeti faktor oblike $8{,}395184144\ldots + o(1)$. To storita s preučevanjem funkcije

$$\gamma(w) := \max \{n \in \mathbb{N} | \, w \in \gamma_n(F_2)\} \cup \{\infty\}.$$

Če namreč definiramo $\gamma_n := \gamma(a_n) = \gamma(b_n)$, se da pokazati zvezo $\gamma_{n+2} - 2\gamma_{n+1} - \gamma_n \geq 0$ za vse $n \in \mathbb{N} \cup \{0\}$, s čimer se da po enakem postopku kot v dokazu 4.15 izračunati spodnjo mejo $\gamma_n \geq C_4(1+\sqrt{2})^n - o(1)$. Avtorja razmislek zaključita z ugotovitvijo, da je namesto eksponenta $\kappa = \log_2(\iota)$ ustrezen $\lambda := \log_{1+\sqrt{2}}(\iota)$.

Da dobimo primerljiv rezultat za rešljive grupe, se moramo precej bolj potruditi. Postopek je opisan v [7, str. 3–4], sklicuje se na lastnosti grup avtomorfizmov nilpotentnih grup, ki jih vložimo v primerne splošne linearne grupe, ki jim lahko dokaj učinkovito ocenimo razred rešljivosti. Ker je jedro te vložitve nilpotentno, se lahko skličemo na izrek [**?**], kar nam zagotovi naslednji izrek (formulacija iz [6, str. 25]).

Izrek 4.19. *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 za vse rešljive grupe moči n ali manj, kjer sta konstanti enaki $C_{10} := 86.321{,}05422\ldots$ in $\lambda := 4{,}331612776\ldots$

5 Enostavne, polenostavne in simetrične grupe

Na prvi pogled se zdi nenavadno obravnavati enostavne in simetrične grupe v istem poglavju. Po strukturi se namreč močno razlikuejo; simetrične grupe imajo bogato strukturo edink (kar nam kažejo recimo izrekih Sylowa), po drugi strani pa enostavne nimajo nobenih pravih netrivialnih. Razlog za takšno obravnavo se skriva v postopku za iskanje kratkih zakonov, ki poteka z uporabo naključnih sprehodov. Ta postopek ni konstruktiven, zgolj pokaže nam obstoj nekega kratkega zakona v grupi, vendar ne poznamo njegove oblike. Naključni sprehodi so se izkazali za ključno orodje pri obravnavi družine enostavnih grup $\mathrm{PSL}_2(q)$, ki bo glavna tema poglavja.

Začnimo z razmislekom o pomembnosti enostavnih grup pri iskanju kratkih zakonov v splošnih grupah. Glavno idejo smo pravzaprav že videli v opombi pod razširitveno lemo 3.7, kjer smo ugotovili, da lahko problem iskanja kratkih zakonov v neki konkretni grupi prevedemo na problem o njeni edinki in kvocientu po tej edinki. To idejo bomo povezali z našim znanjem o rešljivih grupah z uvedbo rešljivega radikala.

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 $S(G) = \mathbf{1}$, rečemo, da je G polenostavna grupa.

Lema 5.2. *Rešljivi radikal je dobro definiran za končne grupe.*

Dokaz. Naj bosta M in N rešljivi edinki končne grupe G. Po četrti točke trditve 4.8 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 $N' \triangleleft G$. Po tretji točki trditve 4.8 sledi, da je N' rešljiva in hkrati strogo večja od $S(G)$, kar je protislovno z definicijo rešljivega radikala. □

Naj bo G poljubna končna grupa. S tvorjenjem kratkega eksaktnega zaporedja

$$\mathbf{1} \to S(G) \to G \to G/S(G) \to \mathbf{1}$$

in uporabo razširitvene leme 3.7 vidimo, da za netrivialna zakona $w_{S(G)}$ in $w_{G/S(G)}$ v grupah $S(G)$ oziroma $G/S(G)$ obstaja netrivialni zakon w_G v grupi G, dolžine

$$l(w_G) \leq l(w_{S(G)})l(w_{G/S(G)}).$$

TODO nekje dodaj razmislek o sporadičnih in enostavnih grupah TODO nekje napiši nekaj o klasifikaciji končnih enostavnih grup

Na straneh 28–31 vira [6] je podan razmislek, kako problem v polenostavnih grupah prevedemo na problem o simetričnih grupah in grupah avtomorfizmov enostavnih grupa. Slednjih se lahko presenetljivo elegantno lotimo s pomočjo Schreierjeve domneve, ki jo bomo formulirali. TODO napiši vsaj kot posledico razširivene leme

Definicija 5.4. Naj bo G grupa in $\mathrm{Aut}(G)$ njena grupa avtomorfizmov. Znano dejstvo je, da je grupa notranjih avtomorfizmov $\mathrm{Inn}(G) = \{x \mapsto gxg^{-1} | \, g \in G\}$ njena edinka. Kvocientu $\mathrm{Out}(G) := \mathrm{Aut}(G)/\,\mathrm{Inn}(G)$ rečemo grupa zunanjih avtomorfizmov grupe G.

Izrek 5.5. *Naj bo G končna enostavna grupa, ki ni Abelova. Potem je grupa* $\mathrm{Out}(G)$ *rešljiva razreda največ* 3.

To domnevo so potrdili z uporabo klasifikacije končnih enostavnih grup. Vprašanje, ali obstaja bolj elementaren dokaz, je še vedno odprto. Glede na to, da se iskanje zakonov v enostavnih grupah močno naslanja na to klasifikacijo, bomo domnevo brez zadržkov uporabili. Naj bo H poljubna enostavna grupa. S tvorjenjem kratkega eksaktnega zaporedja

$$\mathbf{1} \to \mathrm{Inn}(H) \to \mathrm{Aut}(H) \to \mathrm{Out}(H) \to \mathbf{1}$$

in uporabo razširitvene leme 3.7 vidimo, da za netrivialna zakona $w_{\mathrm{Inn}(H)}$ in $w_{\mathrm{Out}(H)}$ v grupah $\mathrm{Inn}(H)$ oziroma $\mathrm{Out}(H)$ obstaja netrivialni zakon $w_{\mathrm{Aut}(H)}$ v grupi $\mathrm{Aut}(H)$, dolžine

$$l(w_{\mathrm{Aut}(H)}) \leq l(w_{\mathrm{Inn}(H)})l(w_{\mathrm{Out}(H)}).$$

Ker je H enostavna, velja $H \cong \mathrm{Inn}(H)$. Za splošno grupo G namreč velja $G/Z(G) \cong \mathrm{Inn}(G)$, v primeru enostavnosti (nekomutativne) grupe pa je center seveda trivialen. Dalje, po Schreierjevi domnevi 5.5 in lemi 4.15 obstaja zakon dolžine $c_3 = 50$, ki je zakon za vse rešljive grupe razreda 3 ali manj. Tako zgornjo enačbo prevedemo na

$$l(w_{\mathrm{Aut}(H)}) \leq 50l(w_H).$$

Ko vse to združimo, dobimo TOOO napiši po komponentah. Zdaj se lotimo posameznih delov te enačbe. Ker je podrobna obravnava spošnih enostavnih grup in simetričnih grup preobsežna za okvir te diplomske naloge, bomo zgolj navedli glavne rezultate in povzeli njihove dokaze.

5.1 Simetrične grupe

5.2 Enostavne grupe

5.3 Grupe $PSL_2(q)$

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

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

V primeru $n = 2$ dobimo so elementi podgrupe $Z(\mathrm{SL}_n(q))$ skalarne 2×2 matrike oblike λI z lastnostjo $\det \lambda I = 1$. To enačbo prevedemo na obliko $(\lambda - 1)(\lambda + 1) = 0$.

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.

Lema 5.7. *Naj bo p praštevilo. Potem ima vsak netrivialni zakon v grupi* $\mathrm{PSL}_2(p)$ *dolžino vsaj 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.

[4]

6 Iskanje zakonov z računalnikom

6.1 Iskanje zakonov za grupe $\mathrm{PSL}_2(q)$

To je tisto kar sem že sprogramiral.

6.2 Iskanje generatorjev zakonov za nilpotentne grupe

[2], še posebej pa [1]

7 Zaključek

Slovar strokovnih izrazov

Literatura

[1] 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.

[2] 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`.

[3] 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].

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

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

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

[7] 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].