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 (TODO, morda [**?**, str. 4]) 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 .

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. TODO □

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.

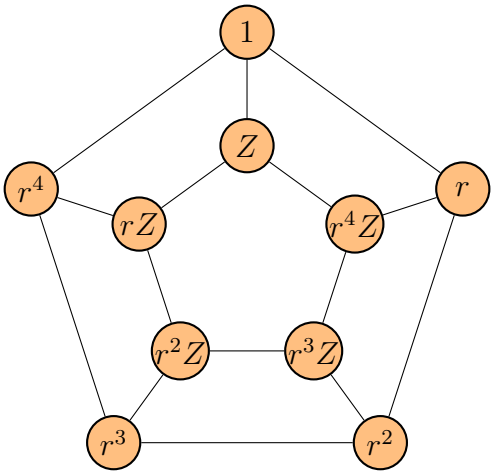
TODO tukaj poveži ožino grafa z bistvom naloge

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



♢

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

Izkaže se, da so najbolj zanimivi zakoni za obravnavo dvočrkovni. To utemeljimo z dokazom naslednje trditve.

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 trditve je naveden v [**?**]. Najprej moramo uvesti nekaj pojmov.

Definicija 2.13. TODO, to se da verjetno izpustiti

Definicija 2.14. TODO

Dokaz. TODO, treba je še prej definirati Schreierjev graf in fundamentalno grupo grafa TODO vstavi sliko fraktalnega drevesa TODO ta dokaz je nekoliko bolj tehničen, kot sem pričakoval, lahko ga tudi samo opišem, ker bi bilo treba definirati veliko pojmov, ki so v nadaljevanju naloge neuporanbni □

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 ([**?**][str. 8, trditev 2.7)**.** *] Naj bo U množica s k-elementi in naj bo $F_k = \langle U \rangle$. Potem je U baza F_k.*

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. Po lemi (TODO citiraj prejšnjo lemo) 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 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 $v_1 \neq v_2^{\pm 1}$, nastavimo $w := [v_1, v_2]$. Po prejšnji lemi (TODO sklicuj se!) je beseda w netrivialna, hkrati pa po (TODO Schutzenbergovi lemi) tudi ni netrivialna potenca. Poleg tega po indukcijski predpostavki velja

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

□

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 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

4 Nilpotentne in rešljive grupe

[?], [?], [?]

5 Enostavne grupe

[?]

6 Grupe $\mathbf{PSL_2(q)}$ in $\mathbf{PSL_n(q)}$

[?], [?]

7 Simetrične grupe

[?]

8 Iskanje zakonov z računalnikom

8.1 Iskanje zakonov za grupe $\mathbf{PSL_2}(q)$

To je tisto kar sem že sprogramiral.

8.2 Iskanje generatorjev zakonov za nilpotentne grupe

[?], še posebej pa [?]

9 Zaključek

Slovar strokovnih izrazov

Literatura

[1] H. Bradford in A. Thom, *Short laws for finite groups of lie type*, 2022, dostopno na `https://arxiv.org/abs/1811.05401`, verzija 5. 10. 2022 [ogled 29. 2. 2024].

[2] 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.

[3] 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`.

[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 Business Media, 2015.

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