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 [5, 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.

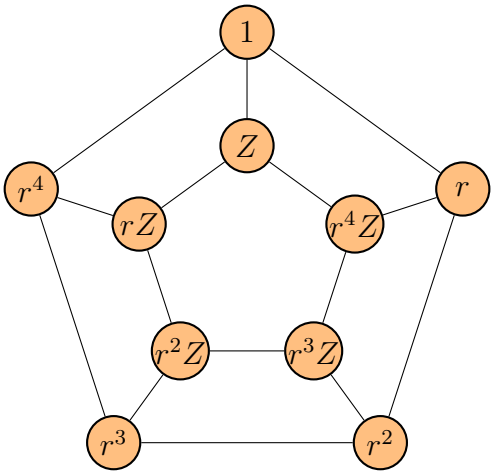
Ime ožina je smiselno v kontekstu definicije Cayleyjevega grafa grupe.

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 množico vozlišč $V = G$ in povezavami $E = \{(p, q) |\, p^{-1}q \in S\}$. Imenujemo ga Cayleyjev graf grupe G, generiran z množico S.

Opomba 2.9. Pogoj $S = S^{-1}$ nam pove, da je $\mathrm{Cay}(G, S)$ res 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 D_{10} (diedrske grupe z 10 elementi) za različni generatorski množici. TODO nariši grafa, enega imaš iz predstaviltve, drugega postavi zraven



□

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

Trditev 2.11. *Obstaja vložitev* $F_{2\cdot 3^k} = \langle x_1, \ldots, x_{2\cdot 3^k} \rangle$ *v* $F_2 = \langle x, y \rangle$*, da velja* $l(x_i) = 2k + 1$*, kjer* $l(w)$ *označuje dolžino besede* $w \in F_2 = \langle x, y \rangle$*.*

Dokaz. TODO, treba je še prej definirati Schreierjev graf in fundamentalno grupo grafa □

3 Komutatorska in razširitvena lema

[6]

4 Nilpotentne in rešljive grupe

[6], [1], [4]

5 Enostavne grupe

[6]

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

[1], [6]

7 Simetrične grupe

[4]

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

[3], še posebej pa [2]

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.