UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Zaključna naloga

Posplošene kvaternionske grupe

(Generalized quaternion groups)

Ime in priimek: Erik Stepančič
študijski program: Matematika
Mentor: izr. prof. dr. István Kovács

Koper, november 2014

Ključna dokumentacijska informacija

Ime in PRIIMEK: Erik STEPANČIČ

Naslov zaključne naloge: Posplošene kvaternionske grupe

Kraj: Koper

Leto: 2014

Število listov: 32 Število slik: 1 Število tabel: 2

Število referenc: 8

Mentor: izr. prof. dr. István Kovács

Ključne besede: grupa, nilpotentna grupa, posplošena kvaterninonska grupa.

Math. Subj. Class. (2010): 20A05, 20D15, 20D25.

Izvleček:
Glavni in najpomembnejši cilj zaključne naloge je izračunati razred nilpotentnosti posplošene kvaternionske grupe Q_{2^n}. Soočili se bomo tudi z različnimi koncepti s področja teorije končnih grup in p-grup. Zaključna naloga je sestavljena iz štirih poglavij. Prvo poglavje je namenjeno uvodu zaključne naloge. V drugem preučujemo temeljne pojme teorije grup. V tretjem bomo analizirali posebne podgrupe grupe Q_{2^n}, tako da bomo poiskali center, komutatorsko in Frattinijevo podgrupo. Četrto poglavje bo namenjeno glavnemu rezultatu, določitvi razreda nilpotentnosti grupe Q_{2^n}.

Key words documentation

Name and SURNAME: Erik STEPANČIČ

Title of final project paper: Generalized quaternion groups

Place: Ǩoper

Year: 2014

Number of pages: 32 Number of figures: 1 Number of tables: 2

Number of references: 8

Mentor: Assoc. Prof. István Kovács, PhD

Keywords: group, nilpotent group, generalized quaternion group.

Math. Subj. Class. (2010): 20A05, 20D15, 20D25.

Abstract:
The main and most imporatant goal of this thesis is to compute the nilpotency class of the generalized quaternion group Q_{2^n}. Different concepts of group and p-group theory will also be of fundamental importance. The thesis is divided into four chapters. The first one contains a short introduction. In the second chapter we review all the basic concepts of group theory which will be used later. In the third chapter we will analyze special subgroups of Q_{2^n} such as its center, commutator subgroup and Frattini subgroup. The fourth chapter is devoted to the main result, the determination of the nilpotency class of Q_{2^n}.

Zahvala

Zahvaljujem se mentorju izr. prof. dr. Istvánu Kovácsu za spodbudo, ideje in pomoč pri nastajanju zaključne naloge. Zahvaljujem se tudi vsem profesorjem, asistentom UP FAMNIT za trud, dobro voljo in vso znanje, ki sem ga pridobil v času študija.

Zahvala gre tudi moji družini za spodbudo, omogočanje in podporo pri študiju. Zahvalil bi se rad še vsem sošolcem, ki so kadarkoli priskočili na pomoč.

Hvala vsem mojim prijateljem, ki so me razumeli in verjeli vame.

Dodatno bi se rad zahvalil Tjaši Jogan, ki mi je vlivala voljo, me tolažila ob neuspehih in bila vedno pripravljena pomagati.

Kazalo vsebine

Kazalo tabel

Kazalo slik

1 Uvod

Leta 1843 je William Rowan Hamilton odkril algebro $\mathbb{H}$ dimenzije 4, katere elementi se imenujejo *kvaternioni* [3]. Zanimive podrobnosti o zgodbi tega odkritja in motivaciji Hamiltona bo bralec našel v predavanju [4]. Algebra $\mathbb{H}$ je definirana kot

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

kjer so vsi simboli i, j in k koren števila -1, in množenje $*$ med njimi je definirano po pravilih: $i * j = k = -j * i$, $j * k = i = -k * j$ in $k * i = j = -i * k$. To implicira takoj, da osem kvaternionov $\pm 1, \pm i, \pm j$ in $\pm k$ tvori grupo glede na operacijo $*$. Ta grupa, ki jo označimo z Q, je znana kot *kvaternionska grupa* [1, 2, 7]. Cela Cayleyjeva tabela grupe Q zgleda takole:

$*$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	1	-1	k	$-k$	$-j$	j
$-i$	$-i$	k	-1	1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	1	-1	i	$-i$
$-j$	$-j$	j	k	$-k$	-1	1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	1	-1
$-k$	$-k$	k	$-j$	j	i	$-i$	-1	1

Tabela 0: Cayleyjeva tabela kvaternionske grupe Q.

Poznejša posplošitev grupe Q je peljala v pomemben razred *posplošenih kvaternionskih grup*, in sicer za naravno število $n \geq 3$ posplošena kvaternionska grupa Q_{2^n} je definirana preko sledeče prezentacije (glej [8]):

$$Q_{2^n} = \langle a, b \mid a^{2^{n-1}} = 1, a^{2^{n-2}} = b^2, b^{-1}ab = a^{-1} \rangle,$$

veljav če je $a = i$ in $b = j$ za $n = 3$ potem je $Q_{2^n} \cong Q$. Te grupe igrajo pomembno vlogo v teoriji končnih grup saj imajo nekatere izredne lastnosti. Na primer, vsaka grupa Q_{2^n} ima ciklično podgrupo indeksa 2 (glej tudi [2, Theorem 12.5.1]); ali Q_{2^n} ima največji možen razred nilpotentnosti, in sicer $n - 1$.

V zaključni nalogi bomo obravnavali posplošene kvaternionske grupe. Naš glavni cilj bo dokazati dejstvo, da ima grupa Q_{2^n} razred nilpotentnosti $n-1$ za vsak n.

Temu dokazu bomo posvetili celo četrto poglavje, kjer si bomo najprej pogledali center diederske grupe, ki bo pripomogel k lažjemu izračunu razreda nilpotentnosti. Glavni izrek v tem poglavju in hkrati tudi v zaključni nalogi, je Izrek 4.6.

Za lažjo pot do dokaza bomo potrebovali znanje nekaterih posebnih podgrup grupe Q_{2^n}. Te bomo določili v tretjem poglavju. Najprej bomo pokazali, kateri elementi pripadajo centru. Poiskali bomo komutatorsko podgrupo in pokazali, kakšna je Frattinijeva podgrupa posplošene kvaternionske grupe.

V drugem poglavju bomo obrazložili osnovne pojme. Najprej bomo v prvem podpoglavju predstavili, kaj sploh je grupa in kaj podgrupa, kakšne grupe poznamo in kaj je to edinka. Predstavili bomo, kaj je to homomorfizem in izomorfizem ter navedli dva primera za lažje razumevanje. Spoznali bomo tudi kvocientne grupe, ki jih bomo v nadaljevanju večkrat uporabili. Posebne podgrupe, kot so center, komutatorska podgrupa, Fratinijeva podgrupa in razne njihove lastnosti bomo obrazložili v tretjem podpoglavju. V zadnjem, četrtem podpoglavju pa bomo definirali kaj je to nilpotentnost in kaj razred nilpotentnosti. Preučili bomo tudi, kaj so to p-grupe in njihove razne lastnosti.

Pri izračunih o grupah v tretjem in četrtem poglavju smo sledili navodilom mentorja I. Kovácsa. Literatura, ki smo jo uporabili pri drugem poglavju, je $[1, 2, 5, 6]$.

2 Osnovni pojmi

Da bi razumeli vsebino zaključne naloge, je nujno potrebno poznavanje grup in njihovih lastnosti. V tem poglavju se bomo seznanili z grupami in delovanji na grupah. Vedno bomo imeli opravka s končnimi grupami. V pomoč so mi prišli stari zapiski s predavanj [5, 6] knjigi [1, 2].

2.1 Grupe, podgrupe, edinke

V prvem podpoglavju bomo najprej definirali najosnovnejše pojme. Pokazali bomo, kakšne lasnosti mora imeti grupa. Pogledali bomo, kakšne podgrupe poznamo in kaj je to edinka.

Definicija 2.1. Grupa je par $(G, *)$, kjer je G množica , $*$ pa zaprta binarna operacija na množici G, za katero veljajo naslednji aksiomi:

- **Asociativnost**
  $(a * b) * c = a * (b * c)$ za $\forall a, b, c \in G$.
- **Identiteta** (nevtralni element)
  Obstaja tak element $e \in G$, za katerega velja, $e * x = x * e = x$ za vsak $x \in G$.
- **Inverz**
  Za vsak $a \in G$ obstaja tak element $a' \in G$, da velja $a * a' = a' * a = e$.

Definicija 2.2. Naj bo G grupa. Podmnožica $H \subseteq G$ je **podgrupa** grupe G, če je zaprta za binarno operacijo grupe G in je sama zase tudi grupa za to isto $*$ binarno operacijo. Oznaka $H \leq G$, H je podgrupa grupe G in $H < G$ oznaka pomeni, da $H \leq G$, ampak $H \neq G$.

Definicija 2.3. Naj bo G grupa in $a \in G$. Podgrupi $\{a^n \mid n \in \mathbb{Z}\}$ grupe G pravimo **ciklična podgrupa**, ki je generirana z elementom a.

Definicija 2.4. Grupa G je **abelska**, če je v grupi G operacija $*$ komutativna.

Definicija 2.5. Elementarno abelova grupa je abelova grupa, v kateri je vsak netrivialni element reda p, kjer je p praštevilo neodvisno od elementa.

Definicija 2.6. Naj bo G grupa in $N \leq G$. N je **edinka** v grupi G (oznaka $N \triangleleft G$), če velja $gNg^{-1} = N$ za vsak $g \in G$. N je edinka tedaj in le tedaj, če se vsak levi odsek ujema z desnim odsekom, če je torej $aN = Na$ za vsak $a \in G$.

Definicija 2.7. Naj bo G grupa in $a \in G$. **Red elementa** a je najmanjše neničelno naravno število $n \in \mathbb{N}$, tako da velja: $a^n = 1$, ($a^n = \underbrace{a \cdot a \cdot a \ldots a}_{n}$.)

Če tak n ne obstaja, potem je red elementa $a = \infty$. Oznaka: $o(a)$.

Definicija 2.8. Naj bo G grupa in $M < G$. Podgrupi M pravimo **maksimalna podgrupa**, če za vsako podgrupo H grupe G velja: če je $M \leq H \leq G$, je $M = H$ ali $H = G$.

2.2 Homomorfizmi in kvocientne grupe

Tukaj bomo definirali in prikazali razne preslikave med grupami. Pokazali bomo, kako dobimo kvocientno grupo ter kaj sta homomorfizem in izomorfizem.

Definicija 2.9. Bijektivna preslikava ali bijekcija je preslikava $f : A \to B$, ki je injektivna in surjektivna hkrati. Pri bijektivni preslikavi je poljuben element množice B slika točno enega elementa množice A, zato v tem primeru obstaja tudi inverzna prelikava $f^{-1} : B \to A$.

Definicija 2.10. Naj bosta G in H grupi. Preslikavi

$$f : G \to H,$$

za katero velja $f(ab) = f(a)f(b)$ pravimo **homomorfizem**. To pomeni, da se produkt poljubnih elementov $a, b \in G$ preslika v produkt ustreznih elementov $f(a), f(b) \in H$.

Definicija 2.11. Naj bo f homomorfizem iz grupe G v grupo H. **Jedro** preslikave f je definiran kot množica :

$$\mathrm{Ker}(f) = \{g \in G : f(g) = 1_H\}.$$

Definicija 2.12. Naj bo $\phi : G \to H$ homomorfizem in naj bo ϕ bijektivna preslikava, potem ϕ imenujemo **izomorfizem** iz grupe G v grupo H, ter pišemo $G \cong H$.

Izrek 2.13. *Naj bo f homomorfizem iz grupe G v grupo H. Potem je* $\mathrm{Ker}(f)$ *edinka v G.*

Dokaz. Izberimo si poljuben $a \in G$ in pokažimo, da je $(\mathrm{Ker}(f))^a \subseteq \mathrm{Ker}(f)$.
Naj bo g poljuben element iz $\mathrm{Ker}(f)$. To pomeni, da lahko zapišemo $a^{-1}ga \in (\mathrm{Ker}(f))^a$.

$$
\begin{aligned}
f(a^{-1}ga) &= f(a^{-1})f(g)f(a) = \\
&= f(a^{-1})1_H f(a) = \\
&= f(a^{-1})f(a) = \\
&= (f(a))^{-1}f(a) = 1_H
\end{aligned}
$$

Torej je $a^{-1}ga \in \mathrm{Ker}(f)$. Zato je $(\mathrm{Ker}(f))^a \subseteq \mathrm{Ker}(f)$, kar pomeni da je $\mathrm{Ker}(f)$ edinka v G. □

Primer 2.14. Naj bo $G = GL(n, \mathbb{R})$, splošna linearna grupa dimenzije n nad $\mathbb{R}$, torej grupa vseh obrnljivih matrik reda n nad poljem $\mathbb{R}$; in naj bo $H = (\mathbb{R} \setminus \{0\}, \cdot)$, multiplikativna grupa neničelnih realnih števil.

Izrek v linearni algebri pravi:

1. $\det(A) \neq 0$ za vsak $A \in G = GL(n, \mathbb{R})$.
2. $\det(AB) = \det(A)\det(B)$ za vsaka $A, B \in G = GL(n, \mathbb{R})$.

Tako lahko vidimo da je preslikava $f : G \to H$ homomorfizem, kjer je f definirana kot $f(A) := \det(A)$ za $\forall A \in G$. preslikava f je homomorfizem ni pa izomorfizem, saj preslikava f ni injektivna (več matrik se preslika v 1). Jedro tega homomorfizma so matrike z determinanto 1, ki tvorijo podgrupo $SL(n, \mathbb{R})$, **posebna linearna grupa dimenzije n nad** $\mathbb{R}$. □

Naslednji primer smo izbrali iz [5, strani 7-8.].

Primer 2.15. Naj bo $G = S_X$, grupa vseh permutacij končne množice X, $H = \{1, -1\}$, in naj bo $f : S_X \to \{1, -1\}$, da je $f(g) = 1$ natanko tedaj, ko je g soda permutacija.

Spomnimo se, permutacija g množice X je soda (liha), če je število sodih ciklov v ciklični dekompoziciji permutacije g sodo (liho). Da pokažemo, da je f res homomorfizem, potrebujemo sledečo lemo:

Lema 2.16. *Za vsako permutacijo g in transpozicijo t v S_X je produkt gt soda permutacija natanko tedaj, ko je g liha permutacija.*

Dokaz. Naj bo $t = (x_1, x_2)$ in naj ima g ciklično dekompozicijo $g = g_1 g_2 \cdots g_n$, kjer ima cikel g_i dolžino k_i za vsak $i \in \{1, \ldots, n\}$. Sedaj imamo dve možnosti:

- x_1 in x_2 pripadata istemu ciklu g_i;
- x_1 in x_2 pripadata različnima cikloma g_i in g_j.

V prvem primeru je permutacija $g_i t$ enaka produktu dveh disjunktnih ciklov dolžine l_1 in l_2, ki imata vsoto $l_1 + l_2 = k_i$. Iz tega sledi, da je razlika med številoma sodih ciklov med permutacijami $g_1, \ldots, g_i, \ldots, g_n$ ter $g_1, \ldots, g_i t, \ldots, g_n$ enaka ± 1.

V drugem primeru je permutacija $g_i g_j t$ enaka enemu ciklu dolžine $k_1 + k_2$. Torej dobimo, da je razlika med številoma sodih ciklov med permutacijami $g_1, \ldots, g_i, \ldots, g_j, \ldots, g_n$ ter $g_1, \ldots, g_i g_j t, \ldots, g_n$ enaka ± 1. Lema 2.16 je s tem dokazana. □

Lema 2.16 implicira, da je preslikava f res homomorfizem. Jedro tega homomorfizma f sestoji iz sodih permutacij in je edinka v S_X. Podgrupa vseh sodih permutacij grupe S_X se imenuje **alternirajoča grupa** množice X, ki jo označimo z A_X. Končajmo primer z dokazom tega dejstva.

Izrek 2.17. *Sode permutacije množice X tvorijo podgrupo grupe S_X.*

Dokaz. Pokazati moramo, da držijo naslednje lastnosti:

1. identiteta id je soda permutacija;
2. če je permutacija g soda, potem je tudi obrat g^{-1} soda permutacija;
3. če sta permutaciji g_1 in g_2 sodi, potem je tudi produkt $g_1 g_2$ soda permutacija.

Trivialno držita 1. in 2. lastnost.

Ker je permutacija g_2 soda, lahko pišemo $g_2 = t_1 t_2 \cdots t_{2n}$ za neke transpozicije $t_i, i \in \{1, \ldots, 2n\}$. Torej velja

$$g_1 g_2 = g_1 t_1 t_2 \cdots t_{2n}.$$

Z uporabo prejšnje leme dobimo, da je permutacija $g_1 t_1$ liha. Sledi, da je permutacija $g_1 t_1 t_2$ soda. Če nadaljujemo na ta način, dobimo, da je permutacija $g_1 t_1 t_2 \ldots t_{2n}$ soda in zato drži tudi 3. lastnost. Izrek 2.17. je dokazan. □

Definicija 2.18. Naj bo G grupa in naj bo $N \leq G$ edinka. Množici levih odsekov, oznaka G/N, pravimo **kvocientna (faktorska) grupa** G kvocientno N, kjer je definirano množenje

$$(aN)(bN) = abN \text{ za vsaka} , b \in G.$$

Definicija 2.19. Naj bo G grupa in N edinka v G. Funkciji

$$f : G \to G/N, \ g \mapsto Ng$$

pravimo **kanonična preslikava** iz grupe G v faktorsko grupo G/N.

Lema 2.20. *Naj bosta $H, K \leq G$. Potem velja:*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Dokaz. Spomnimo se da je $HK = \{hk \,|\, h \in H, k \in K\}$. Naj bo $|H| = r, |K| = s$ in $|H \cap K| = t$. Tedaj ima HK kvečjemu rs elementov. Vendar je možno, da je h_1k_1 enako h_2k_2, za $h_1, h_2 \in H$ in $k_1k_2 \in K$. Če je $h_1k_1 = h_2k_2$, potem je $x = (h_2)^{-1}h_1 = k_2(k_1)^{-1}$. Razberemo lahko, da je $x = (h_2)^{-1}h_1$ in $x = k_2(k_1)^{-1}$. Torej je $x \in H \cap K$ in

$$h_2 = h_1x^{-1} \text{ in } k_2 = xk_1.$$

Po drugi strani, če za $y \in H \cap K$ definiramo $h_3 := h_1y^{-1}$ in $k_3 := yk_1$, potem velja $h_3k_3 = h_1k_1$ za $h_3 \in H$ in $k_3 \in K$. To nam pokaže, da vsak element v HK lahko zapišemo v obliki h_ik_i, $h_i \in H$ in $k_i \in K$, za natančno t parov $(h_i, k_i) \in H \times K$. Sledi, da število elementov v HK je $\frac{rs}{t}$. □

Dokaz naše zadnje leme v tem podpoglavju lahko najdemo na primer v [1].

Lema 2.21. *Naj bosta $H, K \leq G$.*
(i) Če je $N \trianglelefteq G$, potem je NK podgrupa grupe G.
(ii) Če je $N \trianglelefteq G$ in $K \trianglelefteq G$, potem je $N \cap K \trianglelefteq G$.
(iii) Če je $N \trianglelefteq G$ in $K \trianglelefteq G$, potem je $NK \trianglelefteq G$.

2.3 Posebne podgrupe

V tretjem podpoglavju bomo definirali center. Seznanili se bomo tudi z nekaj novimi pojmi, kot so komutator, negeneratorski element in komutatorska podgrupa. Spoznali bomo Frattinijevo podgrupo in nekatere njene lastnosti, ki nam bodo prišle prav v tretjem poglavju.

Definicija 2.22. Naj bo G grupa. **Center grupe** G je množica vseh tistih elementov grupe G, ki komutirajo z vsakim elementom grupe G.

$$Z(G) = \{z \in G \mid zg = gz \text{ za } \forall g \in G\}.$$

Takoj lahko opazimo, da če je G abelova grupa, je očitno $Z(G) = G$.

Primer 2.23. Center splošne linearne grupe $GL(n, \mathbb{R})$.

V tem primeru bomo pokazali, da je

$$Z(GL(n, \mathbb{R})) = \big\{\lambda I_n \mid \lambda \in \mathbb{R}, \lambda \neq 0\big\}, \tag{2.1}$$

kjer I_n označi identično matriko reda n. V našem dokazu bomo uporabili rešitve 10., 15. ter 16. naloge v zapisku [6, Algebra 1].

Najprej se spomnimo, da je **permutacijska matrika** $P(g)$ podane permutacije $g \in S_n$ enaka kvadratni matriki reda n, za katero velja:

$$P(g)_{ij} = \begin{cases} 1 & \text{če} \quad j = i^g, \\ 0 & \text{sicer.} \end{cases}$$

Naša prva trditev je 10. naloga v [6, Algebra].

Lema 2.24. *$P(g)^T = P(g)^{-1}$ za vsako permutacijsko matriko $P(g)$.*

Dokaz. Pišimo P za $P(g)$. Po definicijah lahko izračunamo (i,j)-ti element produkta PP^T kot

$$(PP^T)_{ij} = \sum_{k=1}^{n} P_{ik}(P^T)_{kj} = \sum_{k=1}^{n} P_{ik}P_{jk}.$$

Očitno je, da bo vsak produkt $P_{ik}P_{jk}$ enak 0 ali 1; in je enak številu 1 natanko takrat, ko velja

$$k = i^g = j^g. \tag{2.2}$$

g je permutacija množice $\{1, \ldots, n\}$. Lahko je videti, da pri $i \neq j$ pogoj (2.2) ne drži za nobeno število k, pri $i = j$ drži natančno enkrat in sicer za $k = i^\sigma$. S tem smo dokazali, da je $PP^T = I_n$, in zato $P^T = P^{-1}$. □

Naslednja trditev je 15. naloga v [6, Algebra].

Lema 2.25. *Za vsako matriko A velikosti $n \times n$ in za vsako permutacijo $g \in S_n$,*

$$(P(g)AP(g)^{-1})_{ij} = A_{i^g j^g} \text{ za vsaki}, j \in \{1, \ldots, n\}.$$

Dokaz. Zopet pišimo zopet P za $P(g)$. Po prejšnji lemi $P^{-1} = P^T$, in zato (i,j)-ti element produkta PAP^{-1} dobimo kot:

$$(PAP^{-1})_{ij} = (PAP^T)_{ij} = \sum_{k,l=1}^{n} P_{ik}A_{kl}(P^T)_{lj} = \sum_{k,l=1}^{n} P_{ik}A_{kl}P_{jl}.$$

Po definiciji matrike $P = P(g)$ velja, da je element $P_{ik} = 1$ samo če $k = i^g$ in je enak 0 za vsako drugo vrednost od k; in podobno, $P_{jl} = 1$ samo če $l = j^g$ in je enak 0 za vsako drugo vrednost od l. S tem je lema dokazana. □

Zadnja trditev je 16. naloga v [6, Algebra 1].

Lema 2.26. *Če je $n \geq 2$, potem obstaja $A \in GL(n, \mathbb{R})$, za katero velja $AJ_n \neq J_nA$, kjer J_n označi matriko velikosti $n \times n$, kjer so vsi elementi enaki 1.*

Dokaz. Ena od možnih izbir je

$$A = \begin{pmatrix} 1 & 2 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Potem $(AJ_n)_{11} = 3$, podrugi strani pa $(J_nA)_{11} = 1$, zato je $AJ_n \neq J_nA$. □

Zdaj se lotimo dokazati (2.1). Očitno je, da vsaka matrika oblike $\lambda I_n, \lambda \in \mathbb{R}$ komutira z vsako matriko v grupi $GL(n, \mathbb{R})$. Zaradi tega je dovolj dokazati, da če je $X \in Z(GL(n, \mathbb{R}))$ poljubna matrika, potem je $X = \lambda I_n$ za neko realno število λ.

Pišimo $\lambda = X_{11}$ in $\mu = X_{12}$, in naj bosta i, j poljubni različni števili iz $\{1, \dots, n\}$. Obstaja taka permutacija $g \in S_n$, da velja $1^g = i$ in $2^g = j$. Pišimo P za $P(g)$. Potem je $XP = PX$, saj X pripada centru, in torej je $PXP^{-1} = X$. Z uporabo tega in Leme 2.25. lahko pišemo, da je

$$\lambda = X_{11} = (PXP^{-1})_{11} = X_{1^g 1^g} = X_{ii};$$

in

$$\mu = X_{12} = (PXP^{-1})_{12} = X_{1^g 2^g} = X_{ij}.$$

Tako smo dobili, da je $X = (\lambda - \mu)I_n + \mu J_n$.

Naj bo A matrika predpisana v Lemi 2.26. Ker je $XA = AX$, dobimo da je

$$((\lambda - \mu)I_n + \mu J_n)A = A((\lambda - \mu)I_n + \mu J_n).$$

Iz tega pa sledi, da je $\mu(AJ_n - J_nA) = 0$. Ker $AJ_n - J_nA \neq 0$, glej lemo 2.3.5, je $\mu = 0$, in torej $X = \lambda I_n$. □

Definicija 2.27. Elementu $x^{-1}y^{-1}xy$ grupe G pravimo **komutator** elementov x in y in ga označimo takole :

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

Definicija 2.28. Podgrupi $G' \leq G$, ki je generirana z vsemi komutatorji $x^{-1}y^{-1}xy$, pravimo **komutatorska podgrupa**.

Izrek 2.29. *Faktorska grupa G/G' je abelova grupa. Če je N edinka v G in G/N, je abelova, potem $G' \leq N$.*

Dokaz. Naj $f : G \to G/G'$ označi kanonično preslikavo iz G v grupo G/G', glej definicijo 2.19. Naj bosta $u, v \in G/G'$. Predpostavimo, da $f(x) = u$ in $f(y) = v$ za neka elementa $x, y \in G$. Potem velja $f(x^{-1}y^{-1}xy) = u^{-1}v^{-1}uv$. Ker $x^{-1}y^{-1}xy \in G'$, tudi velja $f(x^{-1}y^{-1}xy) = 1$, in zato je $1 = u^{-1}v^{-1}uv$, iz tega sledi, da je $uv = vu$ in G/G' je abelska.

Sedaj predpostavimo, da je G/N abelska za neko edinko N. Za elemente $x, y \in G$ velja

$$N(x^{-1}y^{-1}xy) = (Nx^{-1})(Ny^{-1})(Nx)(Ny) = N.$$

Tako komutator $x^{-1}y^{-1}xy$ pripada grupi N in zato $G' \leq N$. □

Definicija 2.30. Frattinijeva podgrupa $\Phi(G)$ od poljubne grupe G, je definirana kot presek vseh maksimalnih podgrup v grupi G, če maksimalna grupa obstaja, in $\Phi(G) = G$, sicer.

Definicija 2.31. Elementu x pravimo **negeneratorski element** grupe G, kadarkoli je $G = \langle T, x \rangle$ za neko podmnožico T grupe G, potem je grupa $G = \langle T \rangle$.

Naslednja lastnost je [2, Theorem 10.4.1].

Izrek 2.32. *Če grupa G ni trivialna, potem je Frattinijeva podgrupa $\Phi(G)$ sestavljena iz negeneratorskih elementov grupe G.*

Dokaz. Naj bo $x \in G$. Naj bo M maksimalna podgrupa , ki ne vsebuje x. Potem velja $\langle M, x \rangle = G$, ker M je maksimalna. Po drugi strani $\langle M \rangle = M \neq G$, in to pokaže, da x ni negeneratorski element in zato M vsebuje vse negeneratorske elemente. Tako lahko vidimo, da negeneratorski elementi grupe G spadajo v vse maksimalne podgrupe in vsak negeneratorski element je element v grupi $\Phi(G)$.

Pokazati moramo tudi obratno smer, torej da če je $u \in \Phi(G)$, potem je u negeneratorski element grupe G. Po definiciji $G \neq 1$, torej 1 spada med negeneratorske elemente. Predpostavimo, da je $G = \langle T, u \rangle$, kjer je $T \subset G$. Pokazati želimo, da $\langle T \rangle = G$. Predpostavimo s protislovjem, da je $\langle T \rangle = H \neq G$. Sedaj $u \notin H$, ker $\langle H, u \rangle = G \neq H$. Vemo, da obstaja maksimalna podgrupa K, tako da $H \leq K < G$. Potem $u \notin K$, ker sicer $K = \langle K, u \rangle \geq \langle T, u \rangle = G$ in $K = G$. Sledi, da je K maksimalna podgrupa, ki ne vsebuje u, kjer pridemo v protislovje, saj $u \in \Phi(G)$. Dobimo $\langle T \rangle = G$ in vsak $u \in \Phi(G)$ je negeneratorski element grupe G. □

2.4 Nilpotentnost in p-grupe

V četrtem podpoglavju bomo spoznali, kdaj je grupa nilpotentna in jo bomo bomo tudi natančneje preučili. Seznanili se bomo še s pomenom i-ti center, p-grupe in spoznali njihove lastnosti.

Definicija 2.33. Naj bo $i \in \mathbb{N}$ in G končna grupa. Edinko $Z_i(G) \triangleleft G$, ki jo imenujemo **i-ti center**, definiramo rekurzivno takole:

- $Z_1(G) = Z(G)$.
- če $i > 1$, potem
$$Z_i(G) = \Pi^{-1}(Z(G/Z_{i-1}(G))),$$
kjer Π je kanonična preslikava iz G v $G/Z_{i-1}(G)$.

Definicija 2.34. Grupa G je **nilpotentna**, če $G = Z_n(G)$ za neko $n \in \mathbb{N}$. Najmanjše tako število n imenujemo **razred nilpotentnosti**.

Primer 2.35. Alternirajoča grupa A_4 ni nilpotentna.

Ta grupa je sestavljena iz vseh sodih permutacij množice $\{1, 2, 3, 4\}$, in sicer

$$id, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243).$$

Lahko pokažemo, da vsak element od A_4 oblike $(i\,j)(k\,l)$ komutira samo z elementi $id, (12)(34), (13)(24)$ in $(14)(23)$; in vsak element v obliki $(i\,j\,k)$ komutira samo z elementi $id, (i\,j\,k)$ in $(i\,k\,j)$. Tako smo dobili, da je $Z_1(A_4) = Z(A_4) = \{id\}$.

Zaradi tega $A_4/Z(A_4) = A_4$, in kanonična preslikava $\Pi : A_4 \to A_4/Z(A_4)$ bo v tem primeru le enaka identiteti grupe A_4. Torej, po definiciji 2.4.1 lahko pišemo

$$Z(A_4/Z_1(A_4)) = Z(A_4) = \{id\}, \text{ in zato je } Z_2(A_4) = \Pi^{-1}(\{id\}) = \{\mathrm{id}\}.$$

Lahko nadaljujemo na isti način in dobimo, da je $Z_n(A_4) = \{id\} \neq A_4$ za vsak $n \in \mathbb{N}$, in zato grupa A_4 res ni nilpotentna. □

Izrek 2.36. *Frattinijeva podgrupa $\Phi(G)$ od končne grupe G je nilpotentna.*

Dokaz. Dovolj je pokazati, da je vsaka Sylowa p-podgrupa od $\Phi(G)$ edinka. Naj bo P Sylowa p-podgrupa od $\Phi(G)$. Potem velja $G = \Phi(G)N(P)$, kjer je $N(P)$ normalizator podgrupe P v grupi G. Če $N(P) \neq G$, potem vsaka maksimalna podgrupa grupe G, ki vsebuje $N(P)$, ne more vsebovati Frattinijeve podgrupe $\Phi(G)$. To pa je v nasprotju z definicijo $\Phi(G)$. □

Definicija 2.37. Za dano praštevilo p pravimo, da je grupa P **p-grupa**, če ima vsak netrivialen element grupe P red,ki je potenca števila p.

Izrek 2.38. *Vsaka netrivialna p-grupa G ima netrivialen center.*

Dokaz. Center vsake grupe je unija 1-elementov konjugiranih razredov v grupi. Za p-grupo je velikost vsakega konjugiranega razreda p^n za neko nenegativno celo število n. Netrivialna p-grupa ima tako zmeraj najmanj $p - 1$ netrivialnih konjugiranih razredov (razen 1, ki je zmeraj singleton konjugiranih razredov). Tako lahko vidimo, da je center netrivialen. □

Izrek 2.39. *Če je G p-grupa reda p^n, potem je vsaka maksimalna podgrupa M grupe G reda p^{n-1}.*

Izrek 2.40. *Če je G p-grupa reda p^n, ki je generirana s k elementi, potem je $G/\Phi(G)$ elementarna abelova grupa reda p^k.*

Izrek 2.41. *Vsaka p-grupa je nilpotentna.*

Dokaz. Naj bo G p-grupa. Za $i \in \mathbb{N}$, predpostavimo da je $Z_i(G) < G$. G je končna grupa in obstaja nek n, tako da je $Z_n(G) = Z_{n+1}(G)$. Predpostavimo tudi $Z_n(G) \neq G$. Potem je kvocientna grupa $G/Z_n(G)$ netrivialna p-grupa in po izreku 2.38 nima trivialnega centra. Sledi $Z_{n+1}(G) > Z_n(G)$ in tako pridemo v protislovje. Dobimo $Z_n(G) = G$ in G je nilpotentna po Definiciji 2.34. □

3 Posebne podgrupe grupe Q_{2^n}

V tem poglavju se bomo osredotočili na cilj zaključne naloge in preučili nekaj značilnih podgrup posplošene kvaternionske grupe.

Spomnimo se, da je **posplošena kvaternionska grupa $\mathbf{Q_{2^n}}$**, kjer je $n \geq 3$, definirana takole (glej Uvod):

$$Q_{2^n} = \left\langle a, b \mid a^{2^{n-1}} = 1, a^{2^{n-2}} = b^2, b^{-1}ab = a^{-1} \right\rangle.$$

Lahko opazimo, da je grupa Q_8 izomorfna običajni kvaternionski grupi Q, ki je definirana v Uvodu. To sledi tako iz Tabele 1 in Tabele 2 . Primerjaj obe tabeli. Ker kvaternionska grupa ni komutativna, smo si v tabeli pomagali z izpeljavo:

$$\begin{aligned} b^{-1}ab &= a^{-1} \\ ab &= ba^{-1} \end{aligned}$$

Tako smo dobili $ba = a^3b$, $ba^2 = a^2b$ in $ba^3 = ab$.

$*$	1	a	a^2	a^3	b	ab	a^2b	a^3b
1	1	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	1	ab	a^2b	a^3b	b
a^2	a^2	a^3	1	a	a^2b	a^3b	b	ab
a^3	a^3	1	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	1	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	1	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	1	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	1

Tabela 1: Cayleyjeva tabela grupe Q_8.

V tem poglavju bomo določili tri posebne podgrupe grupe Q_{2^n} in sicer center $Z(Q_{2^n})$, komutatorsko podgrupo Q'_{2^n} ter Frattinejevo podgrupo $\Phi(Q_{2^n})$.

3.1 Center $Z(Q_{2^n})$

Najprej bomo preučili center (glej definicijo 2.22.). V naslednji lemi bomo preučili in spoznali elemente Q_{2^n}, ki nam bodo v pomoč pri iskanju centra.

Lema 3.1. *Grupa Q_{2^n} je reda 2^n, njene elemente lahko zapišemo kot:*

$$1, a, a^2, \dots a^{2^{n-1}-1}, b, ab, a^2b, \dots a^{2^{n-1}-1}b. \tag{3.1}$$

Dokaz. Naj bo A ciklična podgrupa grupe Q_{2^n}, ki je generirana z elementom a, in naj bo B ciklična podgrupa grupe Q_{2^n}, ki je generirana z elementom b. Torej $A = \langle a \rangle$ in $B = \langle b \rangle$. Ker je A edinka, velja $Q_{2^n} = \langle A, B \rangle = AB$. Pokažimo, da veljajo:

$$\mid A \mid = 2^{n-1}, \mid B \mid = 4, \mid A \cap B \mid = 2, |AB| = 2^n$$

1. $\mid A \mid = 2^{n-1}$ sledi iz Definicije 2.4.10
2. $\mid B \mid = 4$. Najprej velja, $b^4 = (b^2)^2 = (a^{2^{n-2}})^2 = a^{2^{n-1}} = 1$.

   Če je $b^k = 1$ potem red elementa b deli k. Red elementa b je lahko $1, 2$ ali 4.

   Ker $b^2 = a^{2^{n-2}} \neq 1$ dobimo, da je $o(b) = 4$ in tako $\mid B \mid = 4$.
3. $\mid A \cap B \mid = 2$ sledi takole, ker je $A \cap B = \{1, b^2 = a^{2^{n-2}}\}$.
4. $|AB| = 2$. Po Lemi 1.2 vemo da

$$|AB| = \frac{|A||B|}{|A \cap B|} = \frac{2^{n-1} \cdot 4}{2} = 2^n.$$

□

Elementi v (3.1) so paroma različni saj tvorijo unijo $A \cup Ab$. Množica A je generirana z elementom a, množica Ab pa je desni odsek grupe A glede na element b. Vidimo lahko, da je $A \cap Ab = \emptyset$. Torej $|A \cup Ab| = 2^n = |Q_{2^n}|$ in tako vidimo, da $Q_{2^n} = A \cup Ab$.

Izrek 3.2. *Center* $Z(Q_{2^n}) = \{1, a^{2^{n-2}}\}$.

Dokaz. Nek element $x \in Z(Q_{2^n}) \Leftrightarrow ax = xa, bx = xb$. Iz prejšnjega dokaza vidimo, da je $ba = a^{-1}b$. To dobimo tako, da

$$\begin{aligned} b^{-1}ab &= a^{-1} \\ ab &= ba^{-1} \\ aba &= b \\ ba &= a^{-1}b. \end{aligned}$$

Sklepamo lahko da je $ba^i = a^{-i}b$. Naslednje enačbe moramo preveriti tako, da namesto x vstavimo $x = a^i$ ali $x = a^ib$, saj bomo tako preverili za vse elemente v Q_{2^n}.

1. Najprej bomo v prvo enačbo $ax = xa$ vstavili $x = a^i$.

$$aa^i = a^i a.$$

   To vemo, da velja saj je množenje v A komutativno.

2. V drugo enačbo $bx = xb$ vstavimo $x = a^i$.

$$\begin{aligned} ba^i &= a^i b \\ a^{-i} b &= a^i b \\ a^{-i} &= a^i \\ a^{2i} &= 1 \\ (a^i)^2 &= 1 \\ i = 0, i = 2^{n-2} &\Rightarrow x_1 = 1, x_2 = a^{2^{n-2}}. \end{aligned}$$

3. V prvo enačbo $ax = xa$ vstavimo $x = a^i b$.

$$\begin{aligned} aa^i b &= a^i ba \\ aa^i b &= a^i a^{-1} b \\ aa^i &= a^i a^{-1} \\ (a^{-1})^2 &= 1. \end{aligned}$$

4. V drugo enačbo $bx = xb$ vstavimo $x = a^i b$.

$$\begin{aligned} ba^i b &= a^i bb \\ a^{-i} bb &= a^i bb \\ (a^i)^2 &= 1 \\ i = 0, i = 2^{n-2} &\Rightarrow x_1 = 1, x_2 = a^{2^{n-2}}. \end{aligned}$$

□

3.2 Komutatorska podgrupa $\mathbf{Q'_{2n}}$

Tukaj bomo pokazali kako izgleda komutatorska podgrupa (glej Podpoglavje 3.2).

Izrek 3.3. *Komutatorska podgrupa* $Q'_{2n} = \langle a^2 \rangle$.

Dokaz. Vemo, da je $A \leq Q_{2^n}$ in red podgrupe A je 2^{n-1}. Pokažimo, da je $A \trianglelefteq Q_{2^n}$, tako da indeks $|Q_{2^n} : A| = 2$.

$$|Q_{2^n} : A| = \frac{|Q_{2^n}|}{|A|} = \frac{2^n}{2^{n-1}} = 2.$$

Vemo, da je $[b, a] = b^{-1}a^{-1}ba = a^2$ in $a^2 \in Q_{2^n}$, torej $\langle a^2 \rangle \leq Q_{2^n}$. Potem je $\langle a^2 \rangle$ edinka. Pokažimo za vsak $x, y \in Q_{2^n} : [x, y] \in \langle a^2 \rangle$, tako da bo element $[x, y] = a^{2l}$ za nek l. Preveriti moramo, da je $x^{-1}y^{-1}xy \in \langle a^2 \rangle$ za 4 primere $x = a^i$ ali $x = a^ib$ in $y = a^j$ ali $y = a^jb$:

1. Najprej bomo vstavili $x = a^i$ in $y = a^j$.

$$a^{-i}a^{-j}a^ia^j = 1 \in \langle a^2 \rangle.$$

2. Vstavimo $x = a^i$ in $y = a^jb$.

$$\begin{aligned}
(a^i)^{-1}(a^jb)^{-1}a^ia^jb &= \\
a^{-i}b^{-1}a^{-j}a^ia^jb &= \\
a^{-i}b^{-1}a^{-j}a^iba^{-j} &= \\
a^{-i}b^{-1}a^{-j}ba^{-i}a^{-j} &= \\
a^{-i}b^{-1}ba^ja^{-i}a^{-j} &= a^{-2i} \in \langle a^2 \rangle.
\end{aligned}$$

3. Vstavimo $x = a^ib$ in $y = a^j$.

$$\begin{aligned}
(a^ib)^{-1}(a^j)^{-1}a^iba^j &= \\
b^{-1}a^{-i}a^{-j}a^iba^j &= \\
b^{-1}a^{-i}a^{-j}ba^{-i}a^j &= \\
b^{-1}a^{-i}ba^ja^{-i}a^j &= \\
b^{-1}ba^ia^ja^{-i}a^j &= a^{2j} \in \langle a^2 \rangle.
\end{aligned}$$

4. Vstavimo $x = a^i b$ in $y = a^j b$.

$$\begin{aligned}
(a^ib)^{-1}(a^jb)^{-1}a^iba^jb &= \\
b^{-1}a^{-i}b^{-1}a^{-j}a^iba^jb &= \\
b^{-1}b^{-1}a^ia^{-j}a^iba^jb &= \\
b^{-1}b^{-1}a^ia^{-j}ba^{-i}a^jb &= \\
b^{-1}b^{-1}a^iba^ja^{-i}a^jb &= \\
b^{-1}b^{-1}ba^{-i}a^ja^{-i}a^jb &= \\
b^{-1}b^{-1}ba^{-i}a^ja^{-i}ba^{-j} &= \\
b^{-1}b^{-1}ba^{-i}a^jba^ia^{-j} &= \\
b^{-1}b^{-1}ba^{-i}ba^{-j}a^ia^{-j} &= \\
b^{-1}b^{-1}bba^ia^{-j}a^ia^{-j} &= a^{2(i-j)} \in \langle a^2\rangle.
\end{aligned}$$

□

3.3 Frattinijeva podgrupa $\Phi(Q_{2^n})$

V tretjem podpoglavju bomo obravnavali Frattinijevo podgrupo. Najprej bomo izračunali lemo, ki nam bo pomagala pri lažjem dokazovanju izreka, da je $\Phi(Q_{2^n}) = \langle a^2\rangle$.

Lema 3.4. *Če je H taka podgrupa v Q_{2^n}, da $\langle a^2\rangle H = Q_{2^n}$, potem je $H = Q_{2^n}$*

Dokaz. Naj bo $H \leq Q_{2^n}$ in $\langle a^2\rangle H = Q_{2^n}$. Za vsak $x \in Q_{2^n}$ $\exists$ $a^{2i} \in \langle a^2\rangle$ in $h \in H$: $a^{2^i}h = x$, za $a^{2i}h = x$. Naj bo $x = a$, potem $\exists i, \exists h$ tako da velja $a^{2i}h = a \Rightarrow h = a^{1-2i}$. Ker je $a^{-2i+1} \in H \Rightarrow \langle a^{-2i+1}\rangle \leq H$ in $\gcd(-2i+1, 2^{n-1}) = 1$, sledi, da je $\langle a\rangle = \langle a^{-2i+1}\rangle \leq H$. Imamo dve možnosti :

- $H = \langle a\rangle$
- $H = \langle a, b\rangle = Q_{2^n}$

Pokazali bomo, da $H = \langle a\rangle$ ni možna, saj je $\langle a^2\rangle H = \langle a^2\rangle\langle a\rangle = \langle a\rangle$ in ta podgrupa ni enaka Q_{2^n} □

Izrek 3.5. *Frattinijeva podgrupa $\Phi(Q_{2^n}) = \langle a^2\rangle$.*

Dokaz. Vemo, da je $\langle a\rangle = A$ maksimalna in $\Phi(Q_{2^n}) \leq \langle a\rangle$. Iz prejšnjega izreka 3.3. smo ugotovili, da je $Q'_{2^n} = \langle a^2\rangle \Rightarrow Q'_{2^n} \lhd Q_{2^n}$. Naj bo $M = \langle a^2\rangle\langle b\rangle$ podgrupa v Q_{2^n}.

$$|M| = \frac{|\langle a^2\rangle||\langle b\rangle|}{|\langle a^2\rangle\langle b\rangle|} = \frac{2^{n-2}\cdot 4}{2} = 2^{n-1}.$$

Izračunamo indeks $|Q_{2^n} : M| = 2 \Rightarrow M$ je tudi maksimalna. Če zelimo pokazati $\Phi(Q_{2^n}) = \langle a^2\rangle$, moramo pokazati $\Phi(Q_{2^n}) \leq \langle a^2\rangle$ in $\Phi(Q_{2^n}) \geq \langle a^2\rangle$.

1. Najprej pokažimo $\Phi(Q_{2^n}) \leq \langle a^2 \rangle$. Vemo da je $\Phi(Q_{2^n}) \leq \langle a \rangle$ in $\Phi(Q_{2^n}) \leq M$, in iz teh sledi, da je
$$\Phi(Q_{2^n}) \leq M \cap \langle a \rangle = \langle a^2 \rangle.$$

2. Pokažimo še, da je $\Phi(Q_{2^n}) \geq \langle a^2 \rangle$. Dovolj, da pokažemo, da je a^2 negeneratorski element, saj potem iz Izreka 2.32. $\Rightarrow a^2 \in \Phi(Q_{2^n})$. Po Definiciji 2.31., a^2 je negeneratorski element $\Leftrightarrow \langle a^2, T \rangle = Q_{2^n} \Rightarrow \langle T \rangle = Q_{2^n}$ za vsako množico T. Naj pišemo $H = \langle T \rangle$. Ker je $\langle a^2 \rangle \lhd Q_{2^n}$, velja
$$\langle a^2, T \rangle = \langle \langle a^2 \rangle, H \rangle = \langle a^2 \rangle H.$$
Vidimo lahko, da je $\langle a^2, T \rangle = Q_{2^n}$ ekvivalentno enakosti $\langle a^2 \rangle H = Q_{2^n}$. Iz Leme 3.4. sledi, da je $\langle T \rangle = H = Q_{2^n}$. Razberemo lahko, da je a^2 res negeneratorski element.

$\square$

4 Razred nilpotentnosti grupe Q_{2^n}

V četrtem poglavju bomo raziskali razred nilpotentnosti grupe Q_{2^n} (glej definicijo 2.34.). Za lažji izračun bomo najprej izračunali center diederske grupe.

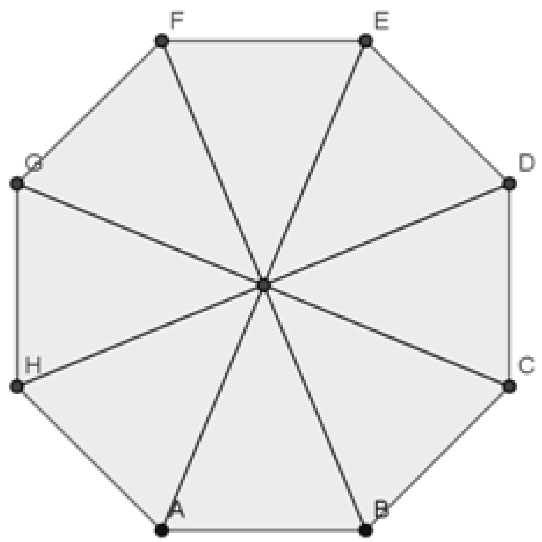
4.1 Center diederske grupe D_{2^n}

Definicija 4.1. Diederska grupa D_{2^n}, kjer je $n \geq 2$, je definirana takole

$$D_{2^n} = \langle a, b | a^{2^{n-1}} = b^2 = 1, b^{-1}ab = a^{-1} \rangle.$$

Opomba 4.2. Diederska grupa D_{2^n} je izomorfna grupi vseh simetrije regularnega 2^{n-1}-kotnika.

Recimo, pravilen 8-kotnik (glej sliko 1) ima skupaj šestnajst simetrij, in sicer 8 rotacij in 8 zrcaljenj. Označimo z G grupo vseh simetrij 8-kotnika.



Slika 1: Pravilni 8-kotnik.

Z ρ bomo označili rotacije v desno s 45 stopinjami okoli centra. Potem lahko vse rotacije dobimo kot :

$$\rho, \rho^2, \rho^3, \rho^4, \rho^5, \rho^6, \rho^7, \rho^8 = id.$$

Naj bo τ zrcaljenje čez premico, ki gre skozi točko F in B. Potem lahko vsa zrcaljenja dobimo kot :

$$\tau, \tau\rho, \tau\rho^2, \tau\rho^3, \tau\rho^4, \tau\rho^5, \tau\rho^6, \tau\rho^7.$$

Torej je grupa G generirana z rotacijami ρ in zrcaljenjem τ. Tudi velja, da je $\tau\rho\tau = \rho^{-1}$. Na koncu lahko pišemo, da je

$$G = \langle \rho, \tau \mid \rho^8 = \tau^2 = 1, \tau\rho\tau = \rho^{-1} \rangle.$$

S tem in definicijo 4.1. lahko vidimo, da je grupa G izomorfna grupi D_{16}.

Lema 4.3. *Naj bo $D_{2^n} = \langle a, b \mid a^{2^{n-1}} = b^2 = 1, bab = a^{-1} \rangle$ in $n \geq 2$. Potem velja*

$$Z(D_{2^n}) = \begin{cases} D_{2^n}, & \text{če } n = 2 \\ \langle a^{2^{n-2}} \rangle, & \text{če } n > 2. \end{cases}$$

Dokaz. Dokaz bomo ločili na dva primera $n = 2$ in $n > 2$:

- Za $n = 2 \Rightarrow D_4 = \langle a, b \rangle = \mathbb{Z}_2 \times \mathbb{Z}_2$ (abelova grupa).
- Za $n > 2$ moramo preveriti še naslednje enačbe $xa = ax$ in $xb = bx$, tako da namesto x vstavimo $x = a^i$ ali $x = a^i b$.

  1. Najprej bomo v prvo enačbo $xa = ax$ vstavili $x = a^i$

  $$\begin{aligned} a^i a &= aa^i \\ a^{i+1} &= a^{i+1} \end{aligned}$$

  2. V drugo enačbo $xb = bx$ vstavimo $x = a^i$.

  $$\begin{aligned} a^i b &= ba^i \\ a^i b &= a^{-i} b \\ a^i &= a^{-i} \\ a^i &= a^{-i} \\ (a^i)^2 &= 1 \\ i = 0, i = 2^{n-2} &\Rightarrow x_1 = 1, x_2 = a^{2^{n-2}}. \end{aligned}$$

3. V prvo enačbo $xa = ax$ vstavimo $x = a^i b$.

$$\begin{aligned} a^i ba &= aa^i b \\ a^i a^{-1} b &= a^i ab \\ a^{i-1} b &= a^{i+1} b \\ a^{i-1} &= a^{i+1} \\ a^{-1} &= a \\ a^2 &= 1, \end{aligned}$$

to nikoli ne velja, saj ima a red $2^{n-1} > 2$, torej $a^2 \neq 1$.

□

4.2 Razred nilpotentnosti grupe Q_{2^n}

V tem podpoglavju bomo vpeljali naš glavni rezultat, in sicer izračun razreda nilpotentnosti grupe Q_{2^n}.

Potrebno je izračunati nekatere faktorske grupe, ki jih dobimo iz grupe Q_{2^n}.

Lema 4.4. *Če $2 \leq i \leq n-1$, potem velja $Q_{2^n}/\langle a^{2^{n-i}} \rangle = D_{2^{n-i+1}}$.*

Dokaz. Naj bo $N = \langle a^{2^{n-i}} \rangle, |N| = 2^{i-1}$.

$$|Q_{2^n}/N| = \frac{2^n}{2^{i-1}} = 2^{n-i+1}.$$

Elementi v Q_{2^n}/N so odseki Nx, Ny, produkt $Nx * Ny = Nxy$. $Q_{2^n} = \langle a, b \rangle \Rightarrow Q_{2^n}/N = \langle Na, Nb \rangle$. Namesto oblike Nx pišemo $\bar{x}$. Grupa Q_{2^n} je definirana kot $\langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, b^{-1}ab = a^{-1} \rangle$. Sedaj moramo izračunati, kako je definirana Q_{2^n}/N. Vedeti moramo, da je $o(a) = 2^{n-1}$ in $o(\bar{a}) = o(Na) = 2^{n-i}$. Najprej bomo izračunali:

$$\bar{a}^{2^{n-i}} = (Na)^{2^{n-i}} = \underbrace{NaNa \ldots Na}_{2^{n-i}} = Na^{2^{n-i}} = N = \bar{1}.$$

Preveriti moramo še za :

$$\bar{b}^2 = (Nb)^2 = Nb^2 = Na^{2^{n-2}} = N = \bar{1}.$$

Torej velja

$$Q_{2^n}/N = \langle \bar{a}, \bar{b} \mid \bar{a}^{2^{n-i}} = 1, \bar{b}^2 = 1, \bar{b}^{-1}\bar{a}\bar{b} = \bar{a}^{-1} \rangle = D_{2^{n-i+1}}.$$

□

Ključni korak je izračunati i-ta center $Z_i(Q_{2^n})$, ko je $1 \leq i \leq n-2$. Spomnimo se, da smo pri $i = 1$ to dobili že v podpoglavju 3.1.

Lema 4.5. *Za $1 \leq i \leq n-2$ velja :*

$$Z_i(Q_{2^n}) = \langle a^{2^{n-i-1}} \rangle.$$

Dokaz. Dokaz bo potekal z indukcijo po i.

1. Najprej bomo pokazali, da velja za $i = 1$.

$$Z_1(Q_{2^n}) = Z(Q_{2^n}) = \langle a^{2^{n-2}} \rangle.$$

   To pa velja saj lahko vidimo iz leme 3.2.

2. Pokazati moramo še, da trditev velja za $i > 1$ in da velja ta enakost:

$$\Pi^{-1}(Z(Q_{2^n}/Z_{i-1}(Q_{2^n}))) = \langle a^{2^{n-i-1}} \rangle,$$

   kjer je Π kanonična preslikava $Q_{2^n} \to Q_{2^n}/Z_{i-1}(Q_{2^n})$.

   Namesto $Z_{i-1}(Q_{2^n})$ lahko pišemo $\langle a^{2^{n-(i-1)-1}} \rangle$. Iz lemme 4.4. sledi, da je

$$Q_{2^n}/Z_{i-1}(Q_{2^n}) = D_{2^{n-i+1}} = \langle \bar{a}, \bar{b} \mid \bar{a}^2 = 1, \bar{b}^2 = \bar{a}^{2^{n-2}}, \bar{b}^{-1}\bar{a}\bar{b} = \bar{a}^{-1} \rangle.$$

   Opazimo lahko, da iz leme 4.3. sledi da je $Z(Q_{2^n}/Z_{i-1}(Q_{2^n})) = \langle \bar{a}^{2^{n-i-1}} \rangle$. Tukaj smo uporabili, da je $n - i + 1 > 2$ $(i \leq n-2)$. Ker Π je kanonična preslikava $Q_{2^n} \to Q_{2^n}/Z_{i-1}(Q_{2^n}) = \langle \bar{a}, \bar{b} \rangle$, velja $\Pi(\langle a^{2^{n-i}} \rangle) = \bar{1}$, in torej

$$\Pi^{-1}(Z(Q_{2^n}/Z_{i-1}(Q_{2^n}))) = \Pi^{-1}(\langle \bar{a}^{2^{n-i-1}} \rangle) = \langle a^{2^{n-i-1}} \rangle.$$

Tako je lema dokazana. □

Izrek 4.6. *Razred nilpotentnosti posplošene kvaternionske grupe Q_{2^n} je enak $n-1$.*

Dokaz. Najprej dobimo iz lemme 4.5., da je

$$Z_{n-2}(Q_{2^n}) = \langle a^{2^{n-(n-2)-1}} \rangle = \langle a^2 \rangle.$$

Zdaj pa izračunamo $Z_{n-1}(Q_{2^n})$.

Naj bo $\Pi : Q_{2^n} \to Q_{2^n}/Z_{n-2}(Q_{2^n})$ kanonična preslikava. Zdaj velja

$$Q_{2^n}/Z_{n-2}(Q_{2^n}) = Q_{2^n}/\langle a^2 \rangle = \langle \bar{a}, \bar{b} \rangle = \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Torej grupa $Q_{2^n}/Z_{n-2}(Q_{2^n})$ je abelova, zato je enaka svojemu centru in dobimo enakost

$$Z_{n-1}(Q_{2^n}) = \Pi^{-1}(Q_{2^n}/Z_{n-2}(Q_{2^n})) = Q_{2^n}.$$

To pa pokaže, da je razred nipotentnosti grupe Q_n res enak $n-1$. □

Končajmo zaključno nalogo z naslednjim izrekom o poljubnih p-grupah.

Izrek 4.7. *Naj bo G neka p-grupa reda p^n in naj $c(G)$ označuje razed nilpotentnosti grupe G. Potem je $c(G) = 1$, če $n = 1$, in*

$$c(G) \leq n - 1, \text{ če } n \geq 2.$$

Zaradi tega lahko izrek 4.6. izrazimo tudi tako, da ima posplošena kvaternionska grupa Q_{2^n} maksimalen razred nilpotentnosti.

5 Zaključek

V zaključni nalogi smo spoznali, kaj so to posplošene kvaternionske grupe Q_{2^n}. Poiskali smo nekatere njihove podgrupe, kot so center, $Z(Q_{2^n})$, komutatorska grupa Q'_{2^n} in Frattinijeva grupa $\Phi(Q_{2^n})$. Vse to je pripomoglo k raziskovanju glavnega cilja zaključne naloge. Dokazali smo, da ima grupa Q_{2^n} razred nilpotentnosti $n-1$ za vsak n. Pri osnovnih pojmih smo navedli dovolj primerov, da bo bralec ležje razumel lažje in prišel do želenega cilja. Seveda obstaja še veliko koristnih in dodatnih informacij, s katerimi lahko poglobimo znanje v dveh knjigah [1] in [2].

6 Literatura

[1] J. B. Fraleigh, *A First course in abstract algebra*, Kingston, Rhode Island: Pearson Education, Inc. 2003. *(Citirano na straneh 1, 2, 3 in 7.)*

[2] M. Hall, Jr., *The theory of groups*, The MAcMillan Co., New York 1959. *(Citirano na straneh 1, 2, 3 in 10.)*

[3] W. R. Hamilton, *On quaternions, or on a new system of imaginaries in algebra*, Philosophical Magazine (1844–1850), edited by D. R. Wilkins, 2000, dostopno na: http://www.emis.ams.org/classics/Hamilton/OnQuat.pdf. *(Citirano na strani 1.)*

[4] J. Huerta, *Introducing The Quaternions*, dostopno na: http://math.ucr.edu/~huerta/introquaternions.pdf. *(Citirano na strani 1.)*

[5] I. Kovács, *Algebra1*, Gradivo 2012, dostopno na: https://e.famnit.upr.si/enrol/index.php?id=114. *(Citirano na straneh 2, 3 in 5.)*

[6] I. Kovács, *Permutacisjke grupe*, Gradivo 2012, dostopno na: https://e.famnit.upr.si/enrol/index.php?id=574. *(Citirano na straneh 2, 3 in 8.)*

[7] E. W. Weisstein, *"Quaternion"*, From MathWorld – A Wolfram Web Resource. http://mathworld.wolfram.com/Quaternion.html. *(Citirano na strani 1.)*

[8] Quaternion group, WikipediA, The Free Encyclopedia. http://en.wikipedia.org/wiki/Quaternion_group *(Citirano na strani 1.)*