UNIVERZA NA PRIMORSKEM

FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

ZAKLJUČNA PROJEKTNA NALOGA

HAMILTONSKE GRUPE

Valentina Petelin

Koper, september 2010

Univerza na Primorskem

Fakulteta za matematiko, naravoslovje in informacijske tehnologije

ZAKLJUČNA PROJEKTNA NALOGA

HAMILTONSKE GRUPE

Valentina Petelin

Mentorica: doc. dr. Klavdija Kutnar

Koper, september 2010

ZAHVALA

Ob tej priložnosti bi se rada zahvalila mentorici doc. dr. Klavdiji Kutnar za podporo, strokovno pomoč, svetovanje in vodenje skozi pripravo zaključne projektne naloge ter za njeno pozitivno energijo skozi vsa leta šolanja. Zahvaljujem se tudi vsem profesorjem na šoli, ki so svoje znanje, izkušnje in strokovnost delili z nami oz. mano.

KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Ime in priimek: Valentina Petelin

Naslov zaključne projektne naloge: Hamiltonske grupe

Kraj: Koper

Leto: 2010

Število strani: 42

Mentorica - predavateljica: doc. dr. Klavdija Kutnar

Prevod v angleščino:

Title: Hamiltonian groups

Povzetek

Namen zaključne projektne naloge je preučiti lastnosti hamiltonskih grup s posebnim poudarkom na osnovnem izreku o hamiltonskih grupah, ki pravi, da je vsaka hamiltonska grupa direktni produkt grupe kvaternionov in torzijske abelove grupe brez elementa reda 4. V nalogi smo najprej obrazložili osnovne pojme s področja algebre, kaj so grupe, podgrupe, podgrupe edinke, homomorfizmi in izomorfizmi grup. Potrebna je bila razlaga kvaternionov, grupe kvaternionov in dedekindovih grup. Primer dedekindovih grup so ciklične in $p-$grupe. Vse to je bilo potrebno, da smo končno lahko definirali hamiltonske grupe in njihovo klasifikacijo. Za konec smo kot zanimivost povedali nekaj o številu hamiltonskih grup.

Ključne besede:

grupa, podgrupa, edinka, abelova grupa, kvaternion, grupa kvaternionov, dedekindova grupa, hamiltonska grupa

Abstract

The purpose of the final research paper is to examine the properties of hamiltonian groups, with particular emphasis on the fundamental theorem of hamiltonian group, which says that every hamiltonian group is a direct product of a the quaternion group and torsion abelian groups without elements of order 4. In this work, we first explain the basic concepts in algebra, such as groups, subgroups, normal subgroups, homomorphisms and isomorphisms. Nessesary was an interpretation of quaternions, quaternion groups, and Dedekind's groups. The examples of Dedekind's groups are cyclic groups and $p-$groups. All that was needed, that we could finally define the hamiltonian groups and their classification. We ended with some facts on the number of hamiltonian groups of a given order.

Keywords:

group, subgroup, normal subgroup, abelian group, quaternion, quaternion group, Dedekind's group, hamiltonian group

Kazalo

Tabele

Slike

Poglavje 1

Uvod

Namen zaključne projektne naloge je preučiti lastnosti hamiltonskih grup, kjer ima pomembno vlogo klasifikacijski izrek o hamiltonskih grupah, ki pravi, da je vsaka hamiltonska grupa direktni produkt grupe kvaternionov in torzijske abelove grupe brez elementa reda 4.

V drugem poglavju bomo na kratko obrazložili osnovne pojme, kaj sploh je grupa z binarno notranjo operacijo v algebri, kakšne grupe poznamo (končne, abelove, enostavne, torzijske, ...), definirali kartezični in direktni produkt, opredelili pojem homomorfizma grup, natančneje izomorfizem, definirali pojem podgrupe. Posebej bomo poudarili podgrupe edinke, saj grupi, katera ima vse podgrupe edinke pravimo dedekindova grupa. Definirali bomo center in centrilizator grupe, saj velja, da je center dane grupe edinka v grupi in obenem tudi abelova grupa. Vsaka abelova grupa je seveda primer dedekindove grupe, obstajajo pa tudi neabelove dedekindove grupe, ki jih imenujemo tako imenovane hamiltonske grupe.

Najmanjši primer hamiltonske grupe je grupa kvaternionov Q_8 (nekateri jo označujejo tudi s K_8), ki je reda 8, zato bomo tretje poglavje namenili tej grupi. Predstavili bomo grupo kvaternionov ter povedali nekaj o Williamu Hamiltonu, ki je odkril grupo Q_8.

V četrtem poglavju bomo namenili nekaj besed matematiku Richardu Dedekindu, ki se je ukvarjal s hamiltonskimi grupami. Preden je prišel do hamiltonskih grup je preučeval abelove grupe, kjer je vsaka podgrupa edinka. Poimenoval jih je po samemu sebi, torej dedekindove grupe. Na kratko bomo predstavili ciklične grupe in $p-$grupe.

Kot smo že omenili obstajajo neabelove dedekindove grupe, ki jih imenujemo hamiltonske grupe. Dedekind je hamiltonske grupe poimenoval po W. Hamiltonu, saj je odkril, da vsebujejo podgrupo reda 8, ki je izomorfna kvaternionski grupi Q_8. O teh pa bomo spregovorili v petem poglavju. Navedli bomo glavni izrek o hamiltonskih grupah (glej izrek 5.6), ga dokazali ter preučili lastnosti hamiltonskih grup.

V zadnjem, šestem poglavju bomo obravnavali število različnih hamiltonskih grup danega reda.

Poglavje 2

Osnovni pojmi

Za začetek naj razložimo nekaj osnovnih pojmov, na katere se bomo kasneje sklicevali.

2.1 Algebrske strukture

Seštevanje in množenje sta osnovni računski operaciji s števili. Zanju veljajo razni zakoni, ki jih pri računanju stalno uporabljamo, ker si tako okrajšamo in olajšamo delo. Ti zakoni so: asociativnost za seštevanje in množenje, komutativnost za seštevanje in množenje ter distributivnost. Zaradi komutativnostnega in asociativnostnega zakona smemo seštevati in množiti števila v poljubnem vrstnem redu.

Kaj pa je pravzaparav seštevanje? I. Vidav pravi, da je seštevanje pravilo, po katerem pripada vsakemu paru števil a, b neko število, namreč *vsota* $a + b$. Podobno je množenje pravilo, seveda drugo kakor pri seštevanju, po katerem pripada vsakemu paru števil a, b neko število, ki ga imenujemo *produkt* ab. Dve števili potrebujemo, če hočemo izračunati vsoto ali produkt. Zato imenujemo seštevanje in množenje binarni (dvočlenski) operaciji.

Pojem računske operacije lahko posplošimo takole: Vzemimo namesto množice realnih števil poljubno množico A. Kartezični produkt $A \times A$ sestoji iz vseh urejenih parov (a, b), kjer sta a in b elementa iz množice A. Denimo, da je dana upodobitev f produkta $A \times A$ v množico A. Upodobitev f pomeni pravilo, po katerem pripada vsakemu urejenemu paru (a, b) elementov iz A neki element c v A. Zaznamujemo ga s $c = f(a, b)$ in ga imenujemo *kompozitum* elementov a in b. Zato lahko rečemo, da določa upodobitev $f : A \times A \to A$ neko binarno (dvočlensko) računsko operacijo. Ta operacija priredi paru (a, b) elementov iz A element $f(a, b)$, ki je tudi v A. Kompozitum $f(a, b)$ lahko krajše zaznamujemo z $a \circ b$ oziroma včasih ab ali tudi $a + b$ in ga v zadnjem primeru imenujemo vsota [7].

Obratno je tudi res. Vsaka binarna operacija v množici A določa neko upodobitev produkta $A \times A$ v A. Upodobitev $A \times A \to A$ dobimo tako, da priredimo elementu $(a, b) \in A \times A$ kompozitum $a \circ b \in A$ kot sliko. Torej lahko rečemo: *Upodobitev kartezičnega produkta $A \times A$ v množico A določa neko binarno računsko operacijo v množici A. Vsaka taka operacija se imenuje notranja operacija množice A.*

Definicija 2.1. *Relacija R oziroma binarna relacija R na množici X je podmnožica kartezičnega produkta $X \times X$. S simboli zapisano: $R \subseteq X \times X$ ali tudi $R \subseteq X^2$.*

Primer:

Za začetek vzemimo operacijo seštevanja na množici naravnih števil: $+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, s predpisom $(a, b) \longmapsto a + b \in \mathbb{N}$. Vstota dveh naravnih števil je naravno število, zato je dana operacija notranja. Sedaj pa vzemimo operacijo deljenja na množici celih števil: $/ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, s predpisom $(a, b) \longmapsto a/b \notin \mathbb{Z}$. Tu pa opazimo, da količnih dveh celih števil ni vedno celo število, zato ta operacija ni notranja.

2.2 Grupoidi in polgrupe

Naj bo dana neka upodobitev produkta $A \times A$ v množico A. Ta upodobitev določa, kakor smo spoznali, binarno operacijo na množici A. Kompozitum $a \circ b$ elementov a in b je element množice A. Včasih bomo kompozitum imenovali produkt in ga pisali ab, včasih pa vsota in jo označili z $a + b$. Nevtralna pisava pa je $a \circ b$ [7].

Definicija 2.2. *Množica A z dano binarno operacijo se imenuje* ***grupoid****.*

Grupoid torej določata množica A in binarna oeracija v A. Če enega od teh podatkov spremenimo, npr. binarno operacijo, dobimo drug grupoid. Grupoid je *asociativen*, če velja: $(a \circ b) \circ c = a \circ (b \circ c)$ za vse elemente $a, b, c \in A$. Kadar pa je pri poljubnih $a, b \in A$ izpolnjena enačba $a \circ b = b \circ a$, je grupoid *komutativen*. Vidav trdi, da v splošnem seveda grupoid ne bo niti asociativen niti komutativen. Tak element e v grupoidu A, da je $a \circ e = a$ za vsak $a \in A$, imenujemo *desni nevtralni element*. Podobno je f *levi nevtralni element*, če je $f \circ a = a$ za vsak $a \in A$.

Definicija 2.3. *Element e je* ***nevtralni elment*** *grupoida A, če velja*

$$a \circ e = e \circ a = a \quad za\ \forall a \in A.$$

Primera:

1. Vzemimo v množici realnih števil operacijo seštevanja. Ta operacija je komutativna in asociativna. Nevtralni element je število 0, saj je $a + 0 = 0 + a = a$ za vsako število $a \in \mathbb{R}$.

2. Odštevanje je neka nadaljna binarna operacija v množici realnih števil. Paru a, b pripada tu razlika $a - b$ kot kompozitum. Ta operacija ni niti komutativna niti asociativna. Število 0 je desni nevtralni element, ker je $a - 0 = a$ za vsak $a \in \mathbb{R}$. Levega nevtralnega elementa pa ni.

Če imenujemo binarno operacijo seštevanje, tako da jo zaznamujemo z $a + b$, nevtralni element imenujemo *nič* in ga označimo z 0. Kadar pa imenujemo v poljubnem grupoidu kompozitum produkt in ga označimo z ab, imenujemo nevtralni element *enota* ali *identiteta* in ga včasih zaznamujemo kar z 1.

Pomembno vlogo imajo grupoidi, v katerih velja asociativnostni zakon, in zato si zaslužijo posebno ime [7].

Definicija 2.4. *Asociativen grupoid se imenuje* ***polgrupa****.*

Če si ogledamo prej navedena zgleda je 1. zgled polgrupa, 2. pa ni, ker za odštevanje ne velja zakon asociativnosti. V polgrupi smemo pri produktu $a \circ b \circ c$ izpustiti oklepaje. Zakaj vseeno je, ali najprej izračunamo kompozitum $a \circ b$ in dobljeni element komponiramo z elementom c, ali pa elment a komponiramo z elementom $b \circ c$.

2.3 Grupe

Grupa je taka polgrupa z enoto, v kateri je vsak element obrnljiv. Zaradi izredne pomembnosti teh struktur navedimo še eksplicitno definicijo grupe [7]:

Definicija 2.5. *Naj bo G množica, ki je neprazna ($G \neq \emptyset$) in $\circ$ binarna notranja operacija na množici G. Potem je $(G, \circ)$ grupa, če velja:*

G1: *Za $\forall a, b, c \in G$ velja: $(a \circ b) \circ c = a \circ (b \circ c)$. (Asociativnost operacije $\circ$.)*

G2: *$\exists e \in G$, tako da za $\forall a \in G$ velja: $a \circ e = e \circ a = a$. (e je nevtralni element za operacijo $\circ$.)*

G3: *Za $\forall a \in G$ $\exists a^{-1} \in G$ tako da velja: $a \circ a^{-1} = a^{-1} \circ a = e$. (Obstoj nasprotnega elementa a^{-1}.)*

Zaradi pogoja G1 je G polgrupa, saj je po definiciji 2.2 G grupoid. Grupoid z lastnostjo asociativnosti dane binarne operacije, pa je po definiciji 2.4 polgrupa. Inverznost dveh elementov je vzajemna. Od tod sledi, da je v grupi element a^{-1} natanko določen z elementom a.

Primer:

Vzemimo množico celih števil $\mathbb{Z}$ in operacijo seštevanja celih števil. Preverimo ali je $(\mathbb{Z}, +)$ grupa. Operacija $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, s predpisom $(a, b) \longmapsto a + b \in \mathbb{Z}$ je notranja, ker je vsota dveh celih števil celo število. Asociativnost seštevanja velja, saj za vse $a, b, c \in \mathbb{Z}$ velja $(a + b) + c = a + (b + c)$. Za seštevanje obstaja nevtralni element 0, ker za vsak $a \in \mathbb{Z}$ velja $a + 0 = 0 + a = a$. In nazadnje obstaja tudi nasprotni element $-a$ elementu a, ker za vsak $a \in \mathbb{Z}$ je $a + (-a) = (-a) + a = 0$. Torej, ker za operacijo $+$ veljajo vsi štirje pogoji, je $(\mathbb{Z}, +)$ grupa.

Grupo določata dva podatka: Množica elementov grupe G in binarna operacija v njej. Ta operacija mora ustrezati pogojem G1, G2 in G3 v definiciji grupe (glej definicijo 2.5). Če enega izmed podatkov spremenimo, dobimo drugo grupo.

V dogovor bomo v nadaljevanju zapis $(G, \circ)$ pisali tudi krajše kar G.

Definicija 2.6. *Naj bo $(G, \circ)$ grupa. Če velja komutativnost za relacijo $\circ$:*

$$\forall a, b \in G : a \circ b = b \circ a,$$

*potem grupi $(G, \circ)$ pravimo **komutativna** ali **abelova grupa**.*

V glavnem izreku 5.6 zaključne naloge nastopajo kar tri različne grupe, zato smo zaradi lažjega razločevanja abelovo grupo označili kar z A.

Obstajajo tudi grupe, ki niso abelove. Imenujemo jih **neabelove grupe**. Najmanjša neabelova grupa, ki je reda 6, je *diedrska grupa* $D_{2\cdot 3}$ oziroma njej izomorfna grupa, tako imenovana *simetrična grupa* S_3.

V nadaljevanju bomo uporabili kartezični produkt in direktni produkt, zato ju sedaj oba definirajmo.

Definicija 2.7. ***Kartezični produkt*** *množic $S_1, S_2, ..., S_n$ je množica vseh urejenih $n-$teric $(a_1, a_2, ..., a_n)$, kjer je $a_i \in S_i$ za $i = 1, 2, ..., n$. Kartezični produkt pišemo kot:*

$$S_1 \times S_2 \times \cdots \times S_n$$

ali

$$\prod_{i=1}^{n} S_i.$$

Sedaj, naj bodo $G_1, G_2, ..., G_n$ grupe in uporabimo multiplikativno notacijo za vse grupne operacije, kakor je to storil Fraleigh. Gledano na G_i kot množice lahko formiramo $\prod_{i=1}^{n} G_i$. Pokažimo, da lahko naredimo $\prod_{i=1}^{n} G_i$ v grupo z binarno operacijo množenja po komponentah.

Izrek 2.8. *Naj bodo $G_1, G_2, ..., G_n$ grupe. Za $(a_1, a_2, ..., a_n)$ in $(b_1, b_2, ..., b_n)$ v $\prod_{i=1}^{n} G_i$, definirajmo operacijo množenja po komponentah:*

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n).$$

Potem je $\prod_{i=1}^{n} G_i$ skupaj s to operacijo grupa, ki jo imenujemo ***direktni produkt*** *grup G_i.*

Dokaz. Naj bo $a_i \in G_i$ in $b_i \in G_i$. Ker je G_i grupa, sledi da je $a_ib_i \in G_i$. Po definirani binarni operaciji na $\prod_{i=1}^{n} G_i$ v izreku, sledi, da je $\prod_{i=1}^{n} G_i$ zaprt za dano binarno operacijo. Zakon asociativnosti v $\prod_{i=1}^{n} G_i$ velja. To dokažemo tako, da uporabimo asociativnost po komponentah:

$$\begin{aligned}
(a_1, a_2, ..., a_n)[(b_1, b_2, ..., b_n)(c_1, c_2, ..., c_n)] &= (a_1, a_2, ..., a_n)(b_1c_1, b_2c_2, ..., b_nc_n) \\
&= (a_1(b_1c_1), a_2(b_2c_2), ..., a_n(b_nc_n)) \\
&= ((a_1b_1)c_1, (a_2b_2)c_2, ..., (a_nb_n)c_n) \\
&= (a_1b_1, a_2b_2, ..., a_nb_n)(c_1, c_2, ..., c_n) \\
&= [(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n)](c_1, c_2, ..., c_n).
\end{aligned}$$

Če je e_i identiteta v G_i, je potem očitno, da je z množenjem po komponentah $(e_1, e_2, ..., e_n)$ identiteta v $\prod_{i=1}^{n} G_i$. Nazadnje, $(a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$ je inverz elementa $(a_1, a_2, ..., a_n)$. Torej je $\prod_{i=1}^{n} G_i$ grupa. □

Grupa ima lahko končno ali neskončno mnogo elementov. V prvem primeru jo imenujemo **končna grupa**, število elementov v končni grupi pa **moč grupe** ali **red grupe**. Moč oziroma red grupe $(G, \circ)$ označimo z $|G|$.

V končni grupi lahko za vsak poljuben element, definiramo **red elementa**. Vzemimo končno grupo G in $a \in G$. Red elementa a je definiran kot najmanjše naravno število n tako, da velja $a^n = e$ tj.

$$red(a) = min\{n \in \mathbb{N} \mid a^n = e\}, \tag{2.1}$$

kjer je e enota v grupi G. V kolikor tak n ne obstaja, pravimo, da je a neskončnega reda to je $red(a) = \infty$. V takem primeru je grupa G **neskončna grupa**. Naj opomnimo, da v 5. poglavju red elementa a krajše označujemo z $o(a)$.

2.3.1 Grupne tabele

Grupna ali Cayleyeva tabela, po britanskem matematiku Arthurju Cayleyu, opisuje strukturo končnih grup. V tabeli so prikazane vse možne kombinacije elementov med seboj, glede na dano operacijo v grupi. Iz tabele lahko takoj razločimo nekatere lastnosti grupe, na primer ali je ali ni abelova grupa, kateri elementi so inverzni elementi določenega elementa, kateri elementi so vsebovani v centru grupe in njegovo velikost.

Naj bo G končna grupa z elementi $e, a, b, ..., x$. Vse produkte po dveh izmed teh elementov zapišimo v obliki tabele:

	e	a	b	c	$\dots$	x
e	e	a	b	c	$\dots$	x
a	a	d	f	g	$\dots$	u
b	b	h	k	l	$\dots$	v
c	c	m	n	p	$\dots$	w
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
x	x	q	r	t	$\dots$	z

Ivan Vidav grupno tabelo razlaga na sledeč način. V prvo celico tabele (tista, ki je v tabeli prazna) ponavadi s simbolom označimo katero binarno operacijo v grupi imamo. Začetna, vodoravna vrsta vsebuje vse elemente $e, a, b, c, ..., x$ grupe G v določenem vrstnem redu. V istem vrstnem redu so ti elementi tudi v prvi navpični vrsti. Produkt dveh elementov stoji na križišču vodoravne vrste, ki se začenja s prvim faktorjem, s tisto navpično vrsto, ki se začenja z drugim faktorjem. Ta tabela povsem določa strukturo grupe G.

Oglejmo si dva primera:

$\underline{Primer1:}$

$*$	a	b	c	d
a	b	d	a	a
b	d	a	c	b
c	a	c	d	b
d	a	b	b	c

$\underline{Primer2:}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

V prvem primeru imamo grupo $G = \{a, b, c, d\}$ z binarno, notranjo operacijo $\circ$. V drugem primeru pa je $(G, +) = (\mathbb{Z}_3, +)$.

Če je grupa abelova, obstaja zelo lepa lastnost grupnih tabel in sicer, da je grupna tabela simetrična glede na glavno diagonalo [7].

Primer: Naj bo $G = \mathbb{Z}_4$.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Opazimo, da je grupna tabela res simetrična glede na glavno diagonalo, torej je grupa $(\mathbb{Z}_4, +)$ abelova grupa.

2.3.2 Podgrupe

Obstajajo grupe, ki so vsebovane v drugih večjih grupah. Fraleigh navaja naslednji primer: grupa $(\mathbb{Z}, +)$, kjer je $+$ običajno seštevanje v $\mathbb{Z}$, je vsebovana v grupi $(\mathbb{Q}, +)$, ta pa je še naprej vsebovana v grupi $(\mathbb{R}, +)$. Ko gledamo na grupo $(\mathbb{R}, +)$, ki vsebuje grupo $(\mathbb{Z}, +)$, je pomembno, da operacija $+$ na elementih m in n, kjer $m, n \in (\mathbb{Z}, +)$ proizvede enak element $m + n$, kot če bi elementa m in n vzeli iz grupe $(\mathbb{R}, +)$. Torej, glede na to opozorilo grupa $(\mathbb{Q}^+, \cdot)$ ni vsebovana v grupi $(\mathbb{R}, +)$. Množica $\mathbb{Q}^+$ je sicer vsebovana v $\mathbb{R}$, ampak poglejmo si operaciji v grupah: $2 \cdot 3 = 6$ v $(\mathbb{Q}^+, \cdot)$, medtem ko je $2 + 3 = 5$ v $(\mathbb{R}, +)$. Pogoj, da je grupa vsebovana v drugi grupi ni le, da je množica prve grupe podmnožica druge, ampak tudi da ima grupna, binarna operacija na podmnožici enake lastnosti, kot če bi vzeli grupno operacijo na celi množici [1].

Definicija 2.9. *Naj bo $(G, \circ)$ grupa. Potem je podmnožica $H \subseteq G$ glede na operacijo $\circ$ **podgrupa** grupe G, če je $(H, \circ)$ grupa. S simboli zapisano: $H \leq G$.*

Podgrupo lahko definiramo tudi na naslednji način:

Trditev 2.10. *Naj bo $(G, \circ)$ grupa, potem je $\emptyset \neq H \subseteq G$ **podgrupa** grupe G, natanko tedaj, ko velja:*

$$\forall a, b \in H : a^{-1}b \in H,$$

kjer je a^{-1} obratni element elementa a.

Dokaz. Če je $H \leq G$ očitno velja, da za poljubna $a, b \in H$ tudi $a^{-1}b \in H$. Za dokaz obrata vzemimo poljuben $a \in H$, ta zagotovo obstaja, saj je $H \neq \emptyset$. Poglejmo kaj se zgodi, če v izraz $a^{-1}b$ vstavimo $b = a$: $a^{-1}a = e \in H$. Torej je e v množici H. Če vstavimo $b = e$, dobimo $a^{-1}e = a^{-1} \in H$. Sledi, da H vsebuje inverzni element vsakega svojega elementa. Nazadnje vzamemo še $b \in H$, ki je poljuben in namesto elementa a vzemimo njegov inverz a^{-1}. To lahko storimo, saj smo v prejšnjem koraku dokazali, da H vsebuje inverz vsakega

elementa iz te množice. Torej poglejmo kaj dobimo: $ab = (a^{-1})^{-1}b \in H$. Nazadnje moramo še preveriti asociativnost operacije $\circ$. Za $\forall a, b, c \in H$ zagotovo velja $(a \circ b) \circ c = a \circ (b \circ c)$, saj je $H \subseteq G$. Množica H torej ustreza pogojem G1, G2 in G3 iz definicije 2.5, zato je H podgrupa grupe G. □

Primera:

1. Naj bo $\mathbb{R}$ aditivna grupa realnih števil in $\mathbb{Z}$ aditivna grupa celih števil. Grupna operacija je obakrat seštevanje. Potem je $\mathbb{Z}$ podgrupa grupe $\mathbb{R}$, s simboli zapisano: $\mathbb{Z} \leq \mathbb{R}$.

2. Soda cela števila sestavljajo grupo za seštevanje, zakaj vsota in razlika sodih števil je sodo število. Označimo grupo sodih celih števil s S. Pri tem štejemo 0 za sodo število. Torej je S podgrupa grupe $\mathbb{Z}$ in grupe $\mathbb{R}$: $S \leq \mathbb{Z}$ ter $S \leq \mathbb{R}$.

Uvedimo še naslednje oznake. Naj bo A poljubna množica elementov grupe G in $a \in G$ poljuben. Množico produktov ax, ko preteče x vse elemente množice A, bomo na kratko označili z aA. Torej

$$aA = \{ax \mid a \in A\}.$$

Podobno je

$$Aa = \{xa \mid a \in A\}$$

množica produktov xa za vse elemente $x \in A$. V komutativni grupi seveda velja $Aa = aA$. Če sta A in B množici elementov grupe G, bomo označili z AB množico produktov xy, kjer preteče x vse elemente množice A in y vse elemente množice B:

$$AB = \{xy \mid x \in A, y \in B\}.$$

Z A^{-1} označimo množico vseh inverznih elementov iz množice A:

$$A^{-1} = \{x^{-1} \mid x \in A\}$$

in z A^n množico produktov n elementov:

$$A^n = \{a_1 a_2 ... a_n \mid a_i \in A\}.$$

Sedaj, ko smo definirali množici A^{-1} in A^n, lahko z njuno pomočjo zapišemo definicijo podgrupe na naslednji način.

Definicija 2.11. *Podmnožica H je podgrupa grupe G, če velja: $H = H^{-1}$ in $H^2 = H$.*

Izrek 2.12. *Naj bosta H in K podgrupi v grupi G. Potem je njun produkt HK podgrupa v G, natanko tedaj ko velja, da je $HK = KH$.*

Dokaz. ($\Rightarrow$) Naj bo $HK \leq G$, potem po definiciji 2.11 velja: $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$ ($\Leftarrow$) Recimo, da je $HK = KH$. Dokazati moramo, da je HK podgrupa v G. Torej poglejmo najprej prvi pogoj iz definicije 2.11: $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$. Predzadnji enačaj velja, ker je $K \leq G$ in po definiciji 2.11 velja $K^{-1} = K$. Podobno velja za H. Še drugi pogoj $(HK)^2 = HKHK = HHKK = H^2K^2 = HK$. Ker sta oba pogoja dokazana, sledi da je produkt HK podgrupa v grupi G. □

S simboli smo podgrupo H grupe G označili na naslednji način: $H \leq G$. Pravimo, da je podgrupa H **prava podgrupa** grupe G in označimo: $H < G$, če velja $H \leq G$ in $H \neq G$. V 5. poglavju v dokazu izreka 5.4 bomo potrebovali izraz maksimalne podgrupe, zato je prav, da najprej definiramo koncept maksimalne podgrupe.

Definicija 2.13. *Naj bo G grupa. Podgrupa H grupe G je **maksimalna podgrupa** grupe G, če $H \neq G$ in v G ne obstaja taka podgrupa K, da je $H < K < G$.*

Izrek 2.14. *(Lagrangev izrek) Naj bo G končna grupa in H njena podgrupa. Potem moč podgrupe H deli moč grupe G. Kvocientu $|G|/|H|$ pravimo **indeks** podgrupe H v grupi G in ga označujemo z $[G : H]$.*

2.3.3 Podgrupe edinke

Obstajajo podgrupe z zelo lepimi lastnostmi, imenujemo jih edinke. Vendar preden podamo definicijo podgrupe edinke, moramo definirati še pojem konjugiranke.

Definicija 2.15. *Naj bo H podmnožica grupe G in $a \in G$. Potem množici*

$$H^a = a^{-1}Ha = \{a^{-1}ha | h \in H\}$$

*pravimo **konjugiranka** množice H z elemetom a.*

Definicija 2.16. *Podgrupa H grupe G je **edinka**, če je enaka vsaki od svojih konjugirank, t.j.*

$$H^a = H$$

za vsak $a \in G$. S simboli predstavljeno: $H \lhd G$.

Naj bo G grupa. Podgrupa $H_1 = G$ je **neprava podgrupa** grupe G. Vsem ostalim podgrupam pa pravimo **prave podgrupe**. Podgrupa $H_2 = \langle e \rangle$, ki vsebuje le nevtralni element e, je **trivialna podgrupa**. Vse ostale podgrupe pa so **netrivialne podgrupe**. Grupa $H_1 = G$ je vedno edinka v G, ker je $aGa^{-1} = G$, prav tako je grupa $H_2 = \langle e \rangle$ edinka v G, saj je $aea^{-1} = aa^{-1} = e$ za vsak $a \in G$. Ker je grupa H_1 neprava podgrupa in obenem edinka, ji lahko pravimo kar **neprava edinka**, grupi H_2, ki je trivialna podgrupa in edinka pa **trivialna edinka**. Lahko se tudi zgodi, da drugih edink sploh ni. V tem primeru pravimo, da je grupa *enostavna*.

Definicija 2.17. *Grupa $G \neq \langle e \rangle$ je **enostavna**, če ne premore pravih netrivialnih edink.*

Grupa je prav gotovo enostavna, kadar ni v njej nobene prave netrivialne podgrupe. Naprimer grupa s praštevilsko močjo nima pravih netrivialnih podgrup in je zato enostavna. Moč podgrupe je namreč deljitelj moči grupe. Praštevilo pa je deljivo samo z 1 in samim seboj, tako da v taki grupi ni pravih podgrup.

Preden navedemo definicijo centra in centrilizatorja omenimo kongruenčno relacijo, saj nam bo centrilizator povedal neko lepo lastnost v povezavi s konjugiranimi si elementi, ki jo bomo potrebovali v 5. poglavju.

Definicija 2.18. *Naj bo $(G, \circ)$ grupa in R ekvivalenčna relacija na G. Če za vse $a, a', b, b' \in G$ velja: če*

$$aRb \text{ (beremo: } a \text{ v relaciji z } b) \text{ in } a'Rb', \text{ velja tudi, da je: } a \circ a'Rb \circ b',$$

*pravimo, da je R **kongruenčna relacija** oz. da je relacija R usklajena z operacijo $\circ$.*

Definicija 2.19. *Naj bo G grupa. Množici*

$$Z(G) = \{x \in G \mid xg = gx, za\ \forall g \in G\}$$

*pravimo **center** grupe G.*

Če je G abelova grupa, je očitno: $Z(G) = G$.
Naslednja trditev pove, da je center grupe vedno podgrupa edinka.

Trditev 2.20. *Naj bo G grupa, potem je $Z(G)$ podgrupa edinka v G in $Z(G)$ je abelova grupa.*

Dokaz. Naj bosta $x, y \in Z(G)$ poljubna. Potem je $x^{-1}y \in Z(G)$, saj velja naslednje: $x^{-1}yg = x^{-1}gy = gx^{-1}y$, prvi enačaj velja, ker je $y \in Z(G)$ in drugi pa, ker je $x \in Z(G)$. Sledi, da je $x^{-1}y \in Z(G)$, torej je po trditvi 2.10 $Z(G) \leq G$. Pokazati moramo še, da je $Z(G) \lhd G$. Zadostuje, če pokažemo, da za vsak $x \in Z(G)$ in vsak $a \in G$ velja: $a^{-1}xa \in Z(G)$. V ta namen naj bo $x \in Z(G)$ poljuben in $a \in G$ tudi poljuben. Za vsak $g \in G$ velja: $ga^{-1}xa = gxa^{-1}a = gx = xg = a^{-1}axg = a^{-1}xag$. Sledi, da je $a^{-1}xa \in Z(G)$, torej je $Z(G) \lhd G$. Nazadnje pokažimo še, da je $Z(G)$ abelova grupa. Naj bosta $x, y \in Z(G)$ poljubna. Potem je $xy = yx$, saj sta $x, y \in Z(G)$. Sledi, da je $Z(G)$ abelova grupa. □

Definicija 2.21. *Naj bo G grupa in $x \in G$. Potem je **centrilizator** elementa $x \in G$ v grupi G množica*

$$C_G(x) = \{g \in G \mid xg = gx\}.$$

Povedano z besedami: Centrilizator elementa $x \in G$ je množica tistih elementov grupe G, ki komutirajo z izbranim elementom $x \in G$. Očitno je, da je centrilizator $C_G(x)$ elementa x podgrupa v grupi G. Velja tudi naslednja vsebovanost med centrom in centrilizatorjem: $Z(G) \subset C_G(x)$ za $\forall x \in G$. Velja tudi zveza $Z(G) = \bigcap_{x \in G} C_G(x)$.

Relacija konjugiranja v grupi G je ekvivalenčna relacija. Pripadajoči ekvivalenčni razredi nam grupo G razdelijo na disjunktne podmnožice. Moč ali kardinalnost posameznega ekvivalenčnega razreda je enaka indeksu centrilizatorja $[G : C_G(x)]$, kjer je x predstavnik tega razreda [3]. Kardinalnost ekvivalenčnega razreda, ki vsebuje centralni element a je enaka 1. Centralni element je element, ki je vsebovan v centru grupe G, t.j. $a \in Z(G)$.

Definicija 2.22. *Centrilizator podmnožice $S \subseteq G$ v grupi G je*

$$C_G(S) = \{g \in G \mid gs = sg\ \forall s \in S\}.$$

Definicija 2.23. *Naj bo H podgrupa grupe G in $a \in G$. Podmnožico*

$$aH = \{ah \mid h \in H\}$$

imenujemo ***levi odsek*** *po podgrupi H v grupi G, podmnožico*

$$Ha = \{ha \mid h \in H\}$$

pa ***desni odsek*** *po podgrupi H v grupi G.*

Izrek 2.24. *Podgrupa H grupe G je edinka natanko tedaj, ko se vsak levi odsek aH ujema z ustreznim desnim odsekom Ha. Torej, natanko tedaj ko je $aH = Ha$ za vsak $a \in G$.*

Dokaz. ($\Rightarrow$) Naj bo H podgrupa edinka. Potem velja $aHa^{-1} = H$ za vsak $a \in G$. Od tod sledi, da je $Ha = (aHa^{-1})a = aH(a^{-1}a) = aHe = aH$. ($\Leftarrow$) Naj bo H taka podgrupa, da je $aH = Ha$ za vsak $a \in G$. Potem je $aHa^{-1} = (aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = He = H$. Ker velja to za vsak $a \in G$, je H edinka in izrek je s tem dokazan. □

Definicija 2.25. *Naj bo G grupa in $a, b \in G$. Potem je* ***komutator*** *elementov a in b definiran takole:*

$$[a, b] = a^{-1}b^{-1}ab.$$

Komutatorska podgrupa *pa je*

$$[G, G] = \langle [a, b] \mid a, b \in G \rangle.$$

Torej komutatorska podgrupa je generirana z vsemi možnimi komutatorji grupe G.

Naj bo G grupa in vzemimo $x, y, z \in G$. O naslednjih osnovnih lastnostih, ki veljajo v grupi G, se lahko prepričamo v knjigi C. P. Miliesa in S. K. Sehgala:

1) $[x, y] = 1$, natanko tedaj, ko je $xy = yx$.

2) $x^y = x[x, y]$.

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

4) $[x, y^{-1}] = [y^x]^{y^{-1}}$ in $[x^{-1}y] = [y, x]^{x^{-1}}$.

5) $[xy, z] = [x, z]^y[y, z]$ in $[x, yz] = [x, z][x, y]^z$.

7) $[x, y]z = z[x^z, y^z]$.

Oglejmo si trditev o komutatorski podgrupi v povezavi z edinakmi:

Trditev 2.26. *Naj bo G grupa. Potem je komutatorska podgrupa $[G, G]$ edinka v G.*

Dokaz. Naj bodo $a, b, g \in G$ poljubni. Potem je $[a, b]^g = g^{-1}[a, b]g = g^{-1}a^{-1}b^{-1}abg = g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg = [a^g, b^g] \in [G, G]$. Ker je $[G, G]$ generirana s komutatorji sledi, da $[G, G] \lhd G$. □

2.3.4 Posebne grupe

Če je $H \lhd G$, množica G/H z operacijo $(aH)(bH) = abH$ tvori grupo. Imenujemo jo **kvocientna grupa** grupe G po podgrupi H.

V 6. poglavju uporabimo izraza elementarno abelova grupa in nilpotent, zato ju definirajmo.

Definicija 2.27. ***Elementarno abelova grupa*** *je abelova grupa, v kateri je vsak netrivialni element reda p, kjer je p praštevilo.*

V 6. poglavju v izreku o hamiltonskih grupah (izrek 5.6) smo zaradi razločnejšega zapisa elementarno abelove grupe označili z E.

Naj bo G grupa. Center $Z(G)$ grupe G je podgrupa edinka. Naj bo $Z_2(G)$ inverzna slika centra $Z(G/Z(G))$ kanonične projekcije $\pi_2 \colon G \to G/Z(G)$. Potem je $Z_2(G)$ edinka v G in vsebuje $Z(G)$. Induktivno definiramo: $Z_1(G) = Z(G)$ in $Z_i(G)$ je inverzna slika centra $Z(G/Z_{i-1}(G))$ glede na ustrezno kanonično projekcijo $\pi_i \colon G \to G/Z_{i-1}(G)$. Dobljeno zaporedje podgrup edink grupe G imenujemo *naraščujoča veriga centrov* grupe G.

Definicija 2.28. *Grupa G je* ***nilpotenta****, če $Z_n(G) = G$ za nek $n \in \mathbb{N}$.*

Če je element končnega reda, mu rečemo tudi **torzijski element**. Obstajajo grupe, katere vsebujejo elemente, ki nimajo neskončnega reda, torej le torzijske elemente. Poglejmo si njihovo definicijo.

Definicija 2.29. ***Torzijska grupa*** *je grupa, katere elementi so vsi končnega reda.*

Očitno so vse končne grupe torzijske, zato si poglejmo primer neskončne torzijske grupe.

Primer:

Vzemimo kvocientno grupo $\mathbb{Q}/\mathbb{Z}$. Poglejmo zakaj je vsak element te grupe končnega reda. Elementi iz grupe $\mathbb{Q}/\mathbb{Z}$ so oblike $\mathbb{Z} + q$, kjer je $q \in \mathbb{Q}$. Naj bo $q = \frac{a}{b}$, kjer sta $a, b \in \mathbb{Z}$, potem je $b(\mathbb{Z} + q) = \mathbb{Z} + qb = \mathbb{Z} + a = \mathbb{Z}$. Torej je element $\mathbb{Z} + q$ reda b.

2.3.5 Homomorfizmi in izomorfizmi

Definicija 2.30. *Naj bosta G in H grupi. Preslikavi*

$$f : G \to H,$$

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

Izrek 2.31. *Naj bo $f : G \to H$ homomorfizem grup. Potem se enota grupe G s homomorfizmom f preslika v enoto grupe H in inverzni element elementa a v inverzni element ustreznega elementa $f(a)$.*

Dokaz. Naj bo e enota v grupi G in e' enota v grupi H. Sliko elementa e označimo z $f(e)$. Za vsak $a \in G$ je $ae = a$. Po enačbi $f(ab) = f(a)f(b)$ sledi, da je $f(a)f(e) = f(a)$. Ker je e' enota v grupi H, velja tudi $f(a)e' = f(a)$ in zato $f(a)f(e) = f(a)e'$. Po pravilu krajšanja dobimo $f(e) = e'$. Torej $f(e)$, slika enote e, je enota v H.

Naj bo a^{-1} inverzni element elementa a, tedaj se $aa^{-1} = e$. Po enačbi $f(ab) = f(a)f(b)$ dobimo $f(a)f(a^{-1}) = f(e)$. Ker smo pravkar ugotovili, da je $f(e)$ enota v H, je $f(a^{-1})$ inverzni element slike $f(a)$. Velja torej $f(a^{-1}) = f(a)^{-1}$. S tem je dokaz zakjučen. □

Posebno pomembni so povratno enolični homomorfizmi oziroma bijektivni homomorfizmi.

Definicija 2.32. *Povratno enolični homomorfizem grupe G na grupo H imenujemo* ***izomorfizem****. Če taka upodobitev med G in H obstaja, pravimo, da sta G in H izomorfni grupi.*

Pri izomorfizmu pripada vsakemu elementu grupe G določen element grupe H kot slika in vsak element iz H je slika natanko enega elementa iz grupe G. Produkt dveh elementov iz G se upodobi v produkt ustraznih elementov iz H. Inverzna upodobitev grupe H na grupo G je tudi izomorfizem. Zato je izomorfizem med dvema grupama vzajemen. Če sta G in H izomorfni grupi, zapišemo to z znaki $G \cong H$ [7].

Kdaj sta dve grupi med seboj izomorfni? Ker je izomorfizem povratno enolična upodobitev, imata končni izomorfni grupi isto število elementov, torej isto moč. Toda grupi z isto močjo nista nujno izomorfni. Oglejmo si primer.

Primer:

Vzemimo dve grupi $G_1 = \mathbb{Z}_4$ ter $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$. Ali sta ti dve grupi izomorfni? Obe sta moči 4: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ in $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. Poglejmo sedaj rede elementov v vsaki grupi: 4-terica redov elementov v $\mathbb{Z}_4$ je (1,2,4,4), 4-terica redov elementov v $\mathbb{Z}_2 \times \mathbb{Z}_2$ pa je (1,2,2,2). Ker se redi elementov med grupama ne ujemajo, si grupi nista izomorfni. Torej $G_1 \ncong G_2$ oziroma $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Poglavje 3

Kvaternioni

V matematiki so kvaternioni številski sistem, nekakšna razširitev kompleksnih števil. Iznašel jih je William Rowan Hamilton, 16. oktobra 1843. Leta in leta je poizkušal iznajti 3-dimenzionalen številski sistem, a brez uspeha. Ko je poizkusil s štirimi dimenzijami namesto treh, je delovalo. Problem je bil v tem, da 3-dimenzionalen sistem sploh ne obstaja. Ideja se mu je porodila, ko je bil namenjen na sestanek v Dublin v Royal Irish Academy, med prečkanjem tako imenovanega Broom-ovega mosta. Tako očaran je bil nad povezavo med kompleksnimi števili in 2-dimenzionalno geometrijo, da je še tisti trenutek izklesal temeljno enačbo

$$i^2 = j^2 = k^2 = ijk = -1 \tag{3.1}$$

v kamen Broom-ovega mostu. Sedaj je v ta spomin na tem mestu postavljena kamnita plošča [5].

Sir William Rowan Hamilton (4. avgust 1805 - 2. september 1865) je bil irski fizik, astronom in matematik, ki je naredil pomembne prispevke h klasični mehaniki, optiki in algebri. Študije mehanskih in optičnih sistemov so privedle, do odkritja novih matematičnih pojmov in tehnik. Njegov največji prispevek je morda preoblikovanje Newtonove mehanike, po novem tako poimenovane Hamiltonske mehanike. V matematiki pa je najverjetneje najbolj znan kot izumitelj kvaternionov.

Množico kvaternionov navadno označujemo s H ali $\mathbb{H}$ ali tudi Q_8. Dogovor: množico kvaternionov bomo označevali s H, saj bomo Q_8 uporabljali kasneje za grupo kvaternionov.

Kvaternion je mogoče zapisati na več načinov:

- kot linearno kombinacijo vsote imaginarnih in realnih komponent, v analogiji kompleksnih števil in sicer

$$H = \{a \cdot 1 + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

- z uporabo 2×2 kompleksnih matrik (I.):

$$H = \{\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = \begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix} \mid z, w \in \mathbb{C}, a, b, c, d \in \mathbb{R}\},$$

  kjer je $\overline{z}$ konjugirano število številu z.

- z uporabo 2×2 kompleksnih matrik (II.):

$$U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ I = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix},\ J = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\ K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

  V tem primeru je U identična matrika in ne I, kot jo navadno označimo. Iz tega zapisa kvaternionov sledijo naslednje zveze: $I^2 = J^2 = K^2 = -U$.

- v $\mathbb{R}^4$ so baze kvaterniona podane na naslednji način:

$$\begin{aligned} i &\equiv \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix} \\ j &\equiv \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \\ k &\equiv \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \\ 1 &\equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

Poleg že omenjene temeljne enačbe: $i^2 = j^2 = k^2 = -1$, za kvaternione veljajo še naslednje zveze, katere so izpeljane iz osnovne enačbe (4.1):

$$ij = -ji = k$$

$$jk = -kj = i$$

$$ki = -ik = j$$

To so vsi možni produkti elementov i, j ter k. S pomočjo teh lahko izpolnimo Cayleyjevo tabelo:

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

Za kvaternione velja zakon asociativnosti, zakon komutativnosti odpade, torej so nekomutativni ter tvorijo grupo, tako imenovano **kvaternionsko grupo**, ki je reda 8. Končnih

grup reda 8 je 5. Dve izmed teh sta neabelovi in kvaternionska grupa je ena izmed teh dveh [6].

Možnih je več ekvivalentnih zapisov te grupe:

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\}$$

$$Q_8 = \langle i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\rangle$$

$$Q_8 = \langle a, b \mid a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1}\rangle$$

Elementi te grupe so: $Q_8 = \{1, i, j, k, -1, -i, -j, -k\}$ oziroma $Q_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$

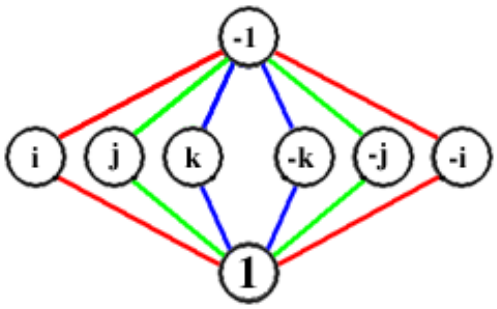
Direktni izračun nam pokaže, da je komutatorska podgrupa enaka $[Q_8, Q_8] = Z(Q_8) = \langle a^2\rangle \cong \mathbb{Z}_2$. Obenem je a^2 edini element v Q_8, ki je reda 2. Torej, če je H katerakoli pripadajoča podgrupa grupe Q_8, sledi, da je $[Q_8, Q_8] = \langle a^2\rangle \leq H$, saj po Cauchyjevem izreku vsaka grupa sodega reda premore element reda 2. Sledi, da je vsaka podgrupa grupe Q_8 edinka. To lahko preverimo, tako da pogledamo vse podgrupe grupe Q_8. Po Lagrangevem izreku 2.14 velja, da ima grupa Q_8 podgrupe moči 1, 2, 4 in 8 in sicer:

$$\begin{aligned} H_1 &= \{1\} \\ H_2 &= \{-1, 1\} \\ H_3 &= \{-1, 1, -i, i\} \\ H_4 &= \{-1, 1, -j, j\} \\ H_5 &= \{-1, 1, -k, k\} \\ H_6 &= \{-1, 1, -i, i, -j, j, -k, k\} \end{aligned}$$

Opazimo, da po definiciji edinke 2.16 za vsako podgrupo velja:

$$\begin{aligned} H_1^q &= H_1 \\ H_2^q &= H_2 \\ H_3^q &= H_3 \\ H_4^q &= H_4 \\ H_5^q &= H_5 \ in \\ H_6^q &= H_6, \end{aligned}$$

kjer je $q \in Q_8$. Torej so res vse podgrupe grupe Q_8 edinke.



Slika 3.1: Ciklični graf grupe kvaternionov.

Slika grafično prikazuje grupo Q_8. Vsaka barva prikazuje serijo redov posamičnega elementa povezanega z identiteto 1. Na primer, rdeč cikel prikazuje $i^2 = -1, i^3 = -i$ in $i^4 = 1$. Obenem ta cikel prikazuje tudi $(-i)^2 = -1, (-i)^3 = i$ in $(-i)^4 = 1$. Podobno velja za ostala dva elementa j in k.

Grupna oziroma Cayleyjeva tabela kvaternionske grupe pa izgleda takole [6]:

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

Poglavje 4

Dedekindove grupe

Julius Wilhelm Richard Dedekind (6. oktober 1831 - 12. februar 1916) je bil nemški matematik, ki je imel pomembno vlogo v abstraktni algebri (zlasti v teoriji kolobarjev), algebrski teoriji števil in temeljih realnih števil.

Ker je v abelovi grupi množenje komutativno, je v tem primeru po definiciji konjugiranja $aHa^{-1} = aa^{-1}H = eH = H$ za vsako podgrupo H in vsak $a \in G$. Torej so v abelovi grupi vse podgrupe edinke.

Trditev 4.1. *Naj bo G abelova grupa, potem je vsaka njena podgrupa tudi edinka.*

Dokaz. Po definiciji edinke moramo dokazati, da za vsak $a \in G$ velja: $H^a = H$. Razpišimo $H^a = \{a^{-1}ha | h \in H\} = \{a^{-1}ah | h \in H\} = \{eh | h \in H\} = \{h | h \in H\} = H$. Prehod iz $a^{-1}ha$ na $a^{-1}ah$ velja zaradi komutativnosti v grupi G, saj je grupa G abelova. □

Definicija 4.2. ***Dedekindova grupa*** *je grupa, v kateri so vse podgrupe edinke.*

Po trditvi 4.1 torej velja, da je vsaka abelova grupa primer dedekindove grupe.

4.1 Ciklične grupe

Definicija 4.3. *Naj bo G grupa in $S \subseteq G$ neka njena podmnožica. Potem najmanjšo podgrupo grupe G, ki vsebuje množico S, imenujemo* ***podgrupa generirana z množico*** *S in označimo $\langle S \rangle$.*

Definicija 4.4. *Grupa G je* ***ciklična****, če jo je moč generirati z enim samim elementom: $G = \langle \{a\} \rangle$ ali krajši zapis $G = \langle a \rangle$.*

Z drugimi besedami grupa je ciklična, če so vsi njeni elementi potence enega izmed njih. Če je $G = \langle a \rangle$, elementu a pravimo *generator* grupe G.

Primer:

Vzemimo grupo $\mathbb{Z}_8$ z operacijo običajnega seštevanja. Ker lahko grupo $\mathbb{Z}_8$ generiramo z elementom 1: $\mathbb{Z}_8 = \langle 1 \rangle$, je dana grupa ciklična.

Vse ciklične grupe so abelove, torej so vse ciklične grupe primeri dedekindovih grup. Vendar pa obrat ne velja. Poljubna abelova grupa ni ciklična [1].

Primer:

Grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ je najmanjši primer abelove grupe, ki ni ciklična. Ta grupa je direktni produkt dveh cikličnih grup moči 2. Njeni elementi so urejeni pari: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$.

Izrek 4.5. *Vsaka ciklična grupa je abelova.*

Dokaz. Naj bo G ciklična grupa in naj bo a generator grupe G: $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Vzemimo dva elementa $g_1, g_2 \in G$. Potem obstajata taki števili r in s, da velja: $g_1 = a^r$ in $g_2 = a^s$. Potem je: $g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1$. Torej grupa G je abelova. □

4.2 p-grupe

Izrek 4.6. *Če je grupa praštevilske moči, je abelova.*

Dokaz. Naj bo moč grupe G praštevilo p: $|G| = p$. Vzemimo $a \in G$, ki ni enota e. Red tega elementa je po Lagrangevem izreku delitelj praštevila p. Toda praštevilo ima le dva delitelja in sicer 1 in p. Red elementa a ni 1, ker $a \neq e$, zato je red enak p. Potence $a^0 = e, a, a^2, \cdots, a^{p-1}$ so si med seboj različne. Ker jih je p, so med njimi vsi elementi grupe G. Grupa G je zato ciklična in kot taka abelova. □

Grupam, katerih red lahko zapišemo kot potenco praštevila p, pravimo *p-grupe*, vendar preden si jih ogledamo, navedimo definicijo razredov konjugiranosti, katere bomo uporabili pri dokazovanju izreka 4.10 in njegove nam pomembne posledice 4.11.

Definicija 4.7. *Ekvivalenčnim razredom relacije kongruiranosti pravimo* ***razredi konjugiranosti***

$$C(g) = \{x^{-1}gx \mid x \in G\}.$$

Razred konjugiranosti elementa g označimo z $C(g)$ ali $[g]$.

Centrilizator $C_G(g)$ elementa $g \in G$ je podgrupa grupe G. Opazimo, da dva različna elementa $x, y \in G$ definirata enak razred konjugiranosti elementa $g \in G$, natanko tedaj, ko je $xgx^{-1} = ygy^{-1}$ oziroma $(x^{-1}y)g(x^{-1}y)^{-1} = g$, kar pomeni, da je $x^{-1}y \in C_G(g)$. Torej velja zveza:

$$|C(g)| = [G : C_G(g)]. \tag{4.1}$$

V primeru, ko je grupa G končna pa velja še:

$$|C(g)| = [G : C_G(g)] = \frac{|G|}{|C_G(g)|}. \tag{4.2}$$

Število razredov konjugiranosti grupe G imenujemo **število razreda**. Naj bo $x_1, \cdots, x_t$ nabor vseh predstavnikov razredov konjugiranosti in naj bo $n_i = |C(x_i)| = [G : C_G(x_i)]$. Ker ti razredi tvorijo disjunktno pokritje grupe G, imamo tako imenovano **enačbo razredov konjugiranosti**:

$$|G| = n_1 + n_2 + \cdots + n_t. \tag{4.3}$$

Spomnimo se še, da je $Z(g) \subset C_G(x_i)$ za $\forall i \in \{1, 2, ..., t\}$. Sledi, da n_i deli indeks $[G : Z(G)]$, $1 \leq i \leq t$. Obenem je tudi $x_i \in G$ centralni element, natanko tedaj, ko je njegov razred konjugiranosti $C(x_i)$ sestavljen natanko iz enega elementa, torej je moči 1. Sledi, da je $|C(g)| = 1$, natanko tedaj, ko je $g \in Z(G)$ in število elementov n_i iz enačbe (4.3), ki so enaki 1, je ravno enako $|Z(G)|$. Torej, lahko zapišemo naslednjo enačbo:

$$|G| = |Z(G)| + \sum_{n_i > 1} n_i.$$

Definicija 4.8. *Grupo reda p^n, kjer je p praštevilo in $n > 0$, imenujemo $p-$**grupa**.*

Velja, da je vsaka elementarno abelova grupa $p-$grupa.

Definicija 4.9. *$p-$**podgrupa** grupe G je podgrupa grupe G, ki je $p-$grupa.*

Naj bo p praštevilo. Element, katerega red je neka potenca praštavila p, torej p^i, kjer je $i > 0$, imenujemo $p-$**element**. V končni $p-$grupi je vsak element $p-$element. Poglejmo si naslednji izrek in njegovo posledico, ki sta osnovni lastnosti $p-$grup.

Izrek 4.10. *Naj bo G netrivialna, končna p-grupa. Potem je $Z(G) \neq \{e\}$.*

Dokaz. Naj bo $|G| = p^n$, za neko pozitivno število n. Dokaz gre s protislovjem. Predpostavimo, da je $Z(G) = \{e\}$. Če to drži, sledi, da je en sam razred konjugiranosti v G sestavljen iz enega samega elementa. Torej, če uporabimo notacijo, kot je v enačbi (4.3), bi veljalo $n_1 = 1$ in $n_i \neq 1$, za $2 \leq i \leq t$. Formula (4.1) nam pokaže, da je vsak $n_i, 2 \leq i \leq t$, deljiv s p. Po enačbi razredov sledi, da je $p^n = 1 + n_2 + \cdots + n_t = 1 + kp$, za neko število k, kar pa je protislovje. □

Nazadnje še posledica izreka 4.10, ki nam je pomembna v tem poglavju.

Posledica 4.11. *Naj bo p praštevilo, potem so vse grupe reda p^2 abelove grupe.*

Dokaz. Naj bo G grupa reda p^2. Izrek 4.10 nam pove, da je $|Z(G)|$ enak bodisi številu p, bodisi številu p^2 in zato sledi, da je indeks $[G : Z(G)]$ bodisi enak p, bodisi 1. Sledi, da je kvocientna grupa $G/Z(G)$ ciklična. Če je $xZ(G)$ generator te grupe, potem je $G = \langle x, Z(G) \rangle$ in ker x komutira z vsakim elementom iz $Z(G)$, sledi da je G abelova. □

Poglavje 5

Hamiltonske grupe

Kot smo že ugotovili, je kvaternionsko grupo moč zapisati na več načinov (glej poglavje 3). V tem poglavju bomo uporabljali naslednji zapis:

$$Q_8 = \langle a, b \mid a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} \rangle$$

Definicija 5.1. *Nekomutativno grupo G, za katero velja, da so vse njene podgrupe edinke, imenujemo* ***hamiltonska grupa****.*

Sedaj bomo podali nekaj lem skupaj z dokazi, ki jih bomo potrebovali v klasifikacijskem izreku hamiltonskih grup, glej izrek 5.6.

Lema 5.2. *Naj bo $H = \langle x, y \rangle$ grupa in naj velja $[x, y] \in Z(H)$. Potem velja:*

(i) $[x^r, y] = [x, y]^r = [x, y^r]$.

(ii) $(xy)^r = x^r y^r [y, x]^{\binom{r}{2}}$.

Dokaz. Prvi del (i) je posledica zvez na strani 21 in sicer:

$$[x^r, y] = x^{-r} y^{-1} x^r y = x^{-r} (x^r)^y = x^{-r} (x^y)^r = x^{-r} (x[x, y])^r = x^{-r} x^r [x, y]^r = [x, y]^r$$

ter

$$\begin{aligned} [x, y^r] &= x^{-1} y^{-r} x y^r = (y^{-r})^x y^r = (y^x)^{-r} y^r = (y[y, x])^{-r} y^r = y^{-r} ([y, x]^{-1})^r y^r = \\ &= y^{-r} [x, y]^r y^r = y^{-r} y^r [x, y]^r = [x, y]^r. \end{aligned}$$

Drugi del (ii), pa dokažemo z indukcijo.

- Za $r = 2$ imamo: $x^2 y^2 [y, x] = x^2 y [y, x] y = (xy)^2$, saj $[y, x] = [x, y]^{-1} \in Z(H)$.
- Sedaj predpostavimo, da za n velja: $(xy)^n = x^n y^n [y, x]^{\binom{n}{2}}$ in si oglejmo:

  $$(xy)^{n+1} = (xy)^n xy = x^n y^n [y, x]^{\binom{n}{2}} xy = x^n y^n xy [y, x]^{\binom{n}{2}}.$$

  Obenem imamo po točki (i)

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

  Nadomestimo to v prejšnjem izrazu in pogledamo kaj dobimo:

  $$(xy)^{n+1} = x^n x y^n [y, x]^n y [y, x]^{\binom{n}{2}} = x^{n+1} y^{n+1} [y, x]^{\binom{n+1}{2}}.$$

  Dobili smo željen rezultat in dokaza je tako konec.

□

Lema 5.3. *(Zornova lema) Naj bo A delno urejena množica. Če ima v množici A vsaka vegiga podmnožic (linearno urejeno zaporedje podmnožic) zgornjo mejo, potem množica A vsebuje maksimalen element.*

Lema 5.4. *Naj bo G abelova p-grupa končnega reda in naj bo $g \in G$ element maksimalnega reda. Potem je $\langle g \rangle$ direktni sumand grupe G, t.j. obstaja $H \leq G$ tako, da je $G = H \times \langle g \rangle$.*

Dokaz. Naj bo $S = \{N \subset G \mid N \leq G, N \bigcap \langle g \rangle = \langle 1 \rangle\}$. V dogovor zaradi lepšega izgleda pišimo $\langle g \rangle = K$. Po Zornovi lemi 5.3 obstaja podgrupa M, ki je maksimalna v S. Če pokažemo, da je $G = MK$, potem bo veljalo $G = M \times K$, kot je željeno. Poskusimo s protislovjem. Predpostavimo, da $G \neq MK$ in vzemimo tak $x \in G \backslash MK$, da je najmanjšega reda. Potem je x^p manjšega reda kot x in zato $x^p \in MK$. Torej je $x^p = yg^l$ za nek $y \in M$ in neko pozitivno število l.

Naj bo $o(g) = p^n$, to pomeni, da je red elementa g enak p^n. Ker je g maksimalnega reda, velja $x^{p^n} = 1$ in ker velja $x^{p^n} = y^{p^{n-1}} g^{lp^{n-1}}$ imamo $g^{lp^{n-1}} = y^{p^{n-1}} \in M \bigcap K = 1$. Torej p deli l, zato pišemo $l = p \cdot l_1$. Sedaj imamo $(xg^{-l_1})^p = y \in M$, ampak $xg^{-l_1} \notin M$, saj $x \notin MK$. Po maksimalnosti podgrupe M v S imamo $\langle xg^{-l_1} \rangle \bigcap K \neq \{1\}$, zato obstaja element $y' \in M$ in pozitivni števili u in k, tako da velja $(xg^{-l_1})^u y' = g^k \neq 1$. Posledično je $(xg^{-l_1})^u \in MK$.
Sedaj poglejmo dve možnosti:

1. možnost: Predpostavimo najprej da velja: $p \mid u$. Potem lahko pišemo $u = p\alpha$ in imamo $(xg^{-l_1})^u = (x^p g^{-pl_1})^\alpha = y^\alpha \in M$. Dobimo $g^k \in M \bigcap K$, kar pa je protislovje.

2. možnost: Sedaj predpostavimo da $p \nmid u$. Potem obstajata taki števili r in s, da velja $1 = rp + su$ in lahko pišemo $x = x^{rp} x^{su}$. Ker velja $o(x^{rp}) < o(x)$ velja, da je $x^{rp} \in MK$ in tudi $x^u \in MK$, nakar pa sledi, da je $x \in MK$, kar pa je protislovje.

Torej, ker smo prišli do protislovja v obeh možnostih, mora biti $G = MK$ oziroma $G = M\langle g \rangle$. □

S klasifikacijo hamiltonskih grup začnemo, tako da pokažemo, da so kvaternionske grupe reda 8 vedno vsebovane v hamiltonskih grupah.

Lema 5.5. *Vsaka hamiltonska grupa vsebuje podgrupo, ki je izomorfna grupi Q_8.*

Dokaz. Naj bo G hamiltonska grupa. Naj bosta x in y elementa iz grupe G, tako da velja $c = [x, y] \neq 1$. Taka elementa obstajata, ker je G neabelova. Velja $\langle x \rangle \lhd G$ in tudi $\langle y \rangle \lhd G$, torej je $c \in \langle x \rangle \bigcap \langle y \rangle$. Vsebovanost v preseku velja, ker je $c = x^{-1}y^{-1}xy = (y^{-1})^x y \in \langle y \rangle$ in $c = x^{-1}y^{-1}xy = x^{-1}x^y \in \langle x \rangle$. Sledi, da obstajata pozitivni števili r in s, tako da je $c = x^r = y^s$. Naj bo $H = \langle x, y \rangle = \langle x \rangle \langle y \rangle$. Enakost $\langle x, y \rangle = \langle x \rangle \langle y \rangle$ velja, ker sta $\langle x \rangle$ in $\langle y \rangle$ edinki v G, saj G hamiltonska grupa. Očitno je $c \in Z(H)$, ker je $c \in \langle x \rangle \bigcap \langle y \rangle$ in $[H, H] = \langle c \rangle$. Ta enakost velja, ker je $H/\langle c \rangle = \langle x\langle c \rangle, y\langle c \rangle \rangle$ abelova (saj $x^{-1}\langle c \rangle y^{-1}\langle c \rangle x\langle c \rangle y\langle c \rangle = x^{-1}y^{-1}xy\langle c \rangle = \langle c \rangle$), je potem $[H, H] \leq \langle c \rangle$. Vendar, ker je $c = [x, y] \in [H, H]$ je zato $[H, H] = \langle c \rangle$. Torej je H nilpotentna grupa s centralnim zaporedjem dolžine 2. Ker je po lemi 5.2 $c^r = [x^r, y] = [c, y] = 1$, sledi, da sta x in y

končnega reda in posledično, ker je $H = \langle x \rangle \langle y \rangle$, je tudi H končega reda. Naj bo $o(x) = m$ in $o(y) = n$. Torej red elementa x je m in red elementa y je n. Privzemimo, da sta x in y izbrana tako, da je vsota $m + n$ minimalna.

Vzemimo praštevilo $p \in \mathbb{Q}$, ki deli m. Ker je $o(x^p) = m/p$, minimalnost vsote $m + n$ implicira, da elementa x^p in y komutirata. Zato je po lemi 5.2 $1 = [x^p, y] = [x, y]^p = c^p$ in zato $o(c) = p$. To pravzaprav pokaže, da morata biti m in n potenci praštevila p. Ker če vzamemo nek dan praštevilsko deljitelj q števila m oziroma n, zopet zaradi minimalnosti dobimo, da je $c^q = 1$ iz česar sledi, da je $q = p$.

Pišimo sedaj $r = kp^{r_1}$ in $s = lp^{s_1}$, tako da je $gcd(p, k) = gcd(p, l) = 1$. Potem obstajata taki števili k' in l', da velja $kk' \equiv 1 \pmod{o(x)}$ in $ll' \equiv 1 \pmod{o(y)}$. Poglejmo, zakaj obstaja tak k'. Ker je $gcd(p, k) = 1$ in $o(x) = p^t$, je potem tudi $gcd(p^t, k) = 1$ in zato $\exists k', b \in \mathbb{Z} : 1 = kk' + bp^t$ oziroma $kk' \equiv 1 \pmod{p}^t = 1 \pmod{o(x)}$. Podobno lahko razložimo zakaj obstaja tak l'. Naj bo $x' = x^{l'}$ in $y' = y^{k'}$. Potem je $[x', y'] = c^{k'l'}$ in $(x')^{p^{r_1}} = x^{l'p^{r_1}} = (x^{p^{r_1}})^{l'}$.

Ker je $c^{k'} = (x^{kp^{r_1}})^{k'} = x^{p^{s_1}}$, imamo $(x')^{p^{r_1}} = c^{k'l'}$. Podobno dobimo za y in sicer $(y')^{p^{s_1}} = c^{k'l'}$. Naj bo $c' = c^{k'l'}$. Potem je $c' = [x', y']$ in $c' = x'^{p^{r_1}} = y'^{p^{s_1}}$. Obenem je tudi $o(x') = p^{r_1+1}$ in $o(y') = p^{s_1+1}$.

Brez škode za splošnost lahko privzamemo, da je $r_1 \geq s_1$. Sedaj izberimo $y_1 = x^{-p^{r_1-s_1}} y \in H$. Potem je

$$[x, y_1] = [x, x^{-p^{r_1-s_1}} y] = [x, y][x, x^{-p^{r_1-s_1}}]^y = [x, y] = c$$

.

Zaradi minimalnosti imamo $o(y_1) \geq p^{s_1+1}$, torej $y_1^{p^{s_1}} \neq 1$. Ampak

$$y_1^{p^{s_1}} = (x^{-p^{r_1-s_1}} y)^{p^{s_1}}$$

in iz (ii) dela leme 5.2 dobimo

$$y_1^{p^{s_1}} = c^{\frac{p^{r_1}(p^{s_1}-1)}{2}}$$

.

Če bi bil p lih, bi potem bil $(p^{s_1} - 1)$ sod in p bi delil število $\frac{p^{r_1}(p^{s_1}-1)}{2}$. Ker smo že pokazali, da je $o(c) = p$, bi moralo veljati $y_1^{p^{s_1}} = 1$, kar pa je protislovje.

Torej, moramo imeti $p = 2$ in $r_1 = 1$, sicer bi z enakim razmislekom dobili $y_1^{p^{s_1}} = 1$.

Ker smo privzeli, da je $r_1 \geq s_1$, sledi, da je $s_1 = 1$ in $o(x') = o(y') = 4$. Sledi torej, da x' in y' ustrezata naslednjim enakostim $x'^4 = 1$, $x'^2 = c = y'^2$ in $[x', y'] = x'^2$. Zadnja enakost je ekvivalentna enakosti $y'^{-1}x'y' = x'^{-1}$. S tem smo pokazali, da je podgrupa $K = \langle x', y' \rangle$ izomorfna grupi Q_8. □

Sedaj, ko smo si ogledali nekaj lem, lahko zapišemo glavno temo zaključne projektne naloge in sicer izrek o hamiltonskih grupah.

Izrek 5.6. *(R. Dedekind, R. Baer) Grupa G je hamiltonska natanko tedaj, ko je G direktni produkt kvaternionske grupe Q_8 reda 8, elementarno abelove 2-grupe E in abelove grupe A, katere vsi elementi so lihega reda.*

Dokaz. Za dokaz potrebnega označimo s $K = \langle x, y \rangle$ podgrupo grupe G, ki je izomorfna grupi Q_8. S simbolnim zapisom: $K \cong Q_8$.
Dokaz je sestavljen iz štirih delov.

1.del: Pokažimo enakost $G = KC_G(K)$.

S protislovjem. Predpostavimo, da obstaja element $g \in G \backslash KC_G(K)$. Potem g ne komutira niti z x, niti z y. Torej $y^g \neq y$. Ker je $y^g \in \langle y \rangle$, saj $\langle y \rangle \lhd G$, sledi, da je $y^g = y^3 = y^{-1}$, torej $o(y^g) = 4$. Potem je $ygx = gy^g x = gy^{-1}x = gx^y y^3 = gx^{-1}x^2 y = gxy$. Predzadnji enačaj velja, ker smo upoštevali, da v K velja, da je $x^2 = y^2$ in da je $x^y = x^{-1}$. Če bi veljalo $(gx)x = x(gx)$, bi bil $gx \in C_G(K) \leq KC_G(K)$, kar pa je v nasprotju z izbiro elementa g. Torej, $(gx)x \neq x(gx)$. Sledi, da je $x^{gx} \neq x$, vendar, ker je $\langle x \rangle \lhd G$ imamo $x^{gx} \in \langle x \rangle$ in zato $x^{gx} = x^{-1}$. Obenem, ker je $x^y = x^{-1}$, imamo $y = x^{-1}yx^{-1}$. Sedaj je $x(gxy) = gxx^{gx}y = gxx^{-1}y = gy = gx^{-1}yx^{-1} = gx^3yx^{-1} = gxy^2yx^{-1} = (gxy)x$, saj $y^2x^{-1} = x^2x^{-1} = x$. Po drugi strani pa je $y(gxy) = y(gx)y = (gxy)y$. Po teh dveh enakostih sledi, da je $gxy \in C_G(K)$, torej je $g \in KC_G(K)$, kar pa je protislovje.

2.del: Pokažimo, da je G torzijska grupa.

Po prvem delu dokaza zadostuje, če pokažemo, da je $C_G(K)$ torzijska. Torej, naj bo g poljuben element iz $C_G(K)$. Potem je $[x, gy] = [x, y][x, g]^y = [x, y] = c \neq 1$. Po dokazu leme 5.5 je gy končnega reda. Sledi, da je tudi g končnega reda.

3.del: Pokažimo, da $C_G(K)$ ne vsebuje elementa reda 4.

Predpostavimo, da obstaja $g \in C_G(K)$, ki je reda 4. Potem, podobno kot prej, $[x, gy] \neq 1$ in $o(gy) = 4$. Torej, je $(gy)^x = (gy)^{-1}$, saj $(gy)^x \in \langle gy \rangle$, saj je $\langle gy \rangle \lhd G$, ker je G hamiltonska. Zato je $(gy)^x = gy$ ali $(gy)^2$ ali $(gy)^3$. Ker je $(gy)^x = x^{-1}gyx = gy^{-1}$, saj $g \in C_G(K)$ in $[x, y] \neq 1$, se lahko hitro prepričamo, da prvi dve možnosti ne nastopita. Zato je $(gy)^x = (gy)^3 = (gy)^{-1}$. Sledi, da je $[gy, x] = (gy)^{-1}(gy)^x = (gy)^{-1}(gy)^{-1} = y^{-1}g^{-1}y^{-1}g^{-1} = g^{-2}y^{-2}$, ker je $g \in C_G(K)$. Po drugi strani pa, kot v lemi 5.5 pridelamo, da je $[gy, x] = (gy)^{-1}x^{-1}gyx = y^{-1}g^{-1}x^{-1}yx = y^{-1}g^{-1}gx^{-1}yx = y^{-1}y^x = y^{-2}$. Ti dve enakosti nam pokažeta, da je $g^2 = 1$, kar pa je protislovje.

4.del: Pokažimo, da je $G = K \times E \times A$, kjer sta E in A grupi navedeni v izreku.

Najprej se spomnimo, da smo pokazali v dokazu leme 5.5, da dva elementa iz G ne komutirata, potem sta 2-elementa. To pomeni, da sta reda 2^i, za nek $i \in \mathbb{N}$. Torej, elementi lihega reda v $C_G(K)$ komutirajo z vsemi elementi iz grupe G. Torej je množica vseh takih elementov A iz G, podgrupa, ki je vsebovana v centru grupe G. Množica A je podgrupa, saj velja, da elementi lihega reda med seboj komutirajo in zato je produkt poljubnih dveh elementov lihega reda zopet element lihega reda.

Po drugi strani pa, če sta g in h dva 2-elementa iz $C_G(K)$, sledi iz tretjega dela, da je $o(x) = o(y) = 2$. Potem je $(xy)^2 = xyxy = xyx^{-1}y$ in ker je $\langle y \rangle$ edinka, sledi, da je $(xy)^2 = y^2 = 1$. Torej je množica B 2-elementov iz $C_G(K)$ elementarno abelova 2-grupa.

Ker je A centralna podgrupa, je očitno $C_G(K) = B \times A$. Obenem, ker je $x^2 \in B$ element maksimalnega reda, sledi po lemi 5.4, da lahko pišemo $B = \langle x^2 \rangle \times E$, kjer je E tudi elementarno abelova 2-grupa. Potem imamo $G = (B \times A)Q_8 = (\langle x^2 \rangle \times E \times A)Q_8 = E \times A \times Q_8$. Iz te zveze sledi, da je tudi E centralna podgrupa.

Da dokažemo obrat, predpostavimo, da je $G = Q_8 \times A \times E$. Zadostovalo bo, da pokažemo, da je za vsak element $g \in G$ podgrupa $\langle g \rangle$ edinka. Pišimo g kot $g = xab$, kjer je $x \in Q_8, a \in$

$A, b \in E$. Če je $o(x) = 2$, potem x pripada centru $Z(G)$ in sledi, da je tudi g v centru $Z(G)$. Če je $o(x) = 4$, je razred konjugiranosti elementa x enak $C(x) = \{x, x^{-1}\}$ in sledi da je razred konjugiranosti elementa g enak $C(g) = \{g, x^{-1}ab\}$. Še vedno moramo pokazati, da je $x^{-1}ab \in \langle g \rangle$. Ker je a lihega reda imamo $s = 2o(a) + 1 \equiv 3 \pmod 4$. Potem je $g^s = x^s a^s b^s = x^{-1}ab$, torej je $x^{-1}ab \in \langle g \rangle$, kot smo želeli.

□

Poglavje 6

Število končnih hamiltonskih grup

Podgrupe abelovih grup so abelovove in obenem tudi edinke. Omenili smo že, da je neabelova grupa, v kateri so vse podgrupe edinke hamiltonska grupa.

B. Horvat, G. Jaklič in T. Pisanski v članku o številu hamiltonskih grup, označijo z A razred abelovih grup in s H razred hamiltonskih grup, zato se bomo v tej zaključni projektni nalogi držali iste notacije. Naj bo $h(n)$ število hamiltonskih grupe reda n in $b(n)$ število grup reda n, katerih lastnost je, da so vse njihove podgrupe edinke. Naj bo $v(n)$ število vseh hamiltonskih grup reda $\leq n$ in $w(n)$ število vseh grup reda $\leq n$, z lastnostjo, da so vse podgrupe teh grup edinke [2].

Spomnimo se strukture končnih abelovih grup [1]. Naj bo $\pi(m)$ particija števila m,

$$\pi(m) := \{m_1, m_2, ..., m_s\},$$

tako da velja: $m = \sum_{k=1}^{s} m_k$ in $m_i \geq m_j$ za vsak $1 \leq i < j \leq s$. Za vsak $c \in \mathbb{N}$ naj bo $c^{\pi(m)} := \{c^{m_1}, c^{m_2}, ..., c^{m_s}\}$ ter naj $A(n_1, n_2, ..., n_r)$ označuje direktni produkt cikličnih grup

$$A(n_1, n_2, ..., n_r) := \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_r}.$$

Naj bo G končna abelova grupa reda n. Praštevilska dekompozicija števila n je:

$$n = \prod_{k=1}^{\ell} p_k^{\alpha_k}.$$

Grupa G je izomorfna grupi $G \cong A(p_1^{\pi(\alpha_1)}, p_2^{\pi(\alpha_2)}, ..., p_\ell^{\pi(\alpha_\ell)})$.

O podanih dejstvih se lahko prepričamo v članku [2].

Naj $a(n)$ označuje število abelovih grup reda n in naj $P(n)$ označuje število particij števila n. Poglejmo si naslednje trditve.

Trditev 6.1. *Število abelovih grup $a(n)$ reda n je enako številu $\prod_{i=1}^{\ell} P(\alpha_i)$, kjer je $n = \prod_{k=1}^{\ell} p_k^{\alpha_k}$.*

O veljavnosti trditve, se lahko prepričamo v knjigi [1].

Prvih 200 vrednosti števila $a(n)$ je podanih v tabeli 6.1.

Tabela 6.1: Začetne vrednosti števila $a(n)$, kjer je $n = 1, 2, ..., 200$.

n	1				5					10						15				20
0	1	1	1	2	1	1	1	3	2	1	1	2	1	1	1	5	1	2	1	2
20	1	1	1	3	2	1	3	2	1	1	1	7	1	1	1	4	1	1	1	3
40	1	1	1	2	2	1	1	5	2	2	1	2	1	3	1	3	1	1	1	2
60	1	1	2	11	1	1	1	2	1	1	1	6	1	1	2	2	1	1	1	5
80	5	1	1	2	1	1	1	3	1	2	1	2	1	1	1	7	1	2	2	4
100	1	1	1	3	1	1	1	6	1	1	1	5	1	1	1	2	2	1	1	3
120	2	1	1	2	3	2	1	15	1	1	1	2	1	1	3	3	1	1	1	2
140	1	1	1	10	1	1	2	2	1	2	1	3	2	1	1	2	1	1	1	7
160	1	5	1	2	1	1	1	3	2	1	2	2	1	1	2	5	1	1	1	4
180	1	1	1	3	1	1	1	2	3	1	1	11	1	1	1	4	1	2	1	6

Razložimo kako se bere podane tabele. Kot smo že omenili, število n pove red grupe. V zgornji tabeli je torej prikazano število abelovih grup od reda 1 pa do 200. Redi se povečujejo od leve proti desni in se nato nadaljujejo v novo vrstico. Se pravi, v prvi vrstici imamo rede grup od 1 do 20, v drugi od 21 do 40, v tretji od 41 do 60, itd. Recimo, da nas zanima koliko je abelovih grup reda 128, v tabeli pogledamo presečišče osmega stolpca in sedme vrstice (120). Z vsoto številke vrstice in številke stolpca moramo pridelati željeno vrednost: $120 + 8 = 128$. Torej, abelovih grup reda 128 je: $a(128) = 15$.

Poglejmo si primer: $24 = 2^3 \cdot 3^1$ in $375 = 3^1 \cdot 5^3$. Obe števili imata praštevilsko oznako (3,1), torej je $a(375) = a(24)$.

Podobna struktura velja za hamiltonske grupe. Hamiltonska grupa H je izomorfna direktnemu produktu kvaternionske grupe Q_8 reda 8, splošni abelovi grupi E z eksponentom 2 ter abelovi grupi A lihega reda

$$H \cong Q \times E \times A \cong Q \times \mathbb{Z}_{2^k} \times A,$$

kjer je $\mid Q_8 \mid = 8 = 2^3$, $\mid E \mid = 2^k$ in $\mid A \mid \neq 0 \pmod 2$. Torej je $\mid H \mid = 2^{3+k} \mid A \mid$.

Naj bo n neko poljubno naravno število. Potem lahko n na enoličen način zapišemo kot $n = 2^e \cdot o$, kjer je $e = e(n) \geq 0$ in $o = o(n)$ neko liho število. Ti rezultati nam dajo število hamiltonskih grup reda n [2].

Trditev 6.2. *Naj bo $n = 2^e \cdot o$, kjer je $e = e(n) \geq 0$ in $o = o(n)$ neko liho število. Število $h(n)$ hamiltonskih grup reda n je dano s formulo*

$$h(n) = \begin{cases} 0, & e(n) < 3; \\ a(o(n)), & \textit{sicer.} \end{cases}$$

Prvih 200 vrednosti števila $h(n)$ je podanih v tabeli 6.2.

Tabela 6.2: Začetne vrednosti števila $h(n)$, kjer je $n = 1, 2, ..., 200$.

n	1				5				10						15					20
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
20	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
40	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
60	0	0	0	1	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	1
80	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
100	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
120	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
140	0	0	0	2	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
160	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
180	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	2

Združevanje vseh hamiltonskih in abelovih grup reda n, katere imajo vse podgrupe edinke, nam ne da števila $b(n) := a(n) + h(n)$. Prvih 300 vrednosti števila $b(n)$ je podanih v spodnji tabeli 6.3.

Tabela 6.3: Začetne vrednosti števila $b(n)$, kjer je $n = 1, 2, ..., 300$.

n	1				5				10						15					20
0	1	1	1	2	1	1	1	4	2	1	1	2	1	1	1	6	1	2	1	2
20	1	1	1	4	2	1	3	2	1	1	1	8	1	1	1	4	1	1	1	4
40	1	1	1	2	2	1	1	6	2	2	1	2	1	3	1	4	1	1	1	2
60	1	1	2	12	1	1	1	2	1	1	1	8	1	1	2	2	1	1	1	6
80	5	1	1	2	1	1	1	4	1	2	1	2	1	1	1	8	1	2	2	4
100	1	1	1	4	1	1	1	6	1	1	1	6	1	1	1	2	2	1	1	4
120	2	1	1	2	3	2	1	16	1	1	1	2	1	1	3	4	1	1	1	2
140	1	1	1	12	1	1	2	2	1	2	1	4	2	1	1	2	1	1	1	8
160	1	5	1	2	1	1	1	4	2	1	2	2	1	1	2	6	1	1	1	4
180	1	1	1	4	1	1	1	2	3	1	1	12	1	1	1	4	1	2	1	8
200	1	1	1	2	1	1	2	6	1	1	1	2	1	1	1	12	1	1	1	2
220	1	1	1	8	4	1	1	2	1	1	1	4	1	2	1	2	1	1	1	6
240	1	2	7	2	2	1	1	4	1	3	1	4	1	1	1	23	1	1	1	2
260	2	1	1	1	1	1	1	2	1	3	1	6	1	1	2	2	1	1	2	4
280	1	1	1	2	1	1	1	16	2	1	1	2	1	2	1	1	3	1	1	4

Število $u(n)$ predstavlja število vseh abelovih grup, ki so reda $\leq n$. Prvih 100 vrednosti števila $u(n)$ je prikazanih v tabeli 6.4.

Tabela 6.4: Začetne vrednosti števila $u(n)$, kjer je $n = 1, 2, ..., 100$.

n	1				5					10
0	1	2	3	5	6	7	8	11	13	14
10	15	17	18	19	20	25	26	28	29	31
20	32	33	34	37	39	40	43	45	46	47
30	48	55	56	57	58	62	63	64	65	68
40	69	70	71	73	75	76	77	82	84	86
50	87	89	90	93	94	97	98	99	100	102
60	103	104	106	117	118	119	120	122	123	124
70	125	131	132	133	135	137	138	139	140	145
80	150	151	152	154	155	156	157	160	161	163
90	164	166	167	168	169	176	177	179	181	185

Naj bo $v(n)$ število hamiltonskih grup reda $\leq n$ in naj bo $w(n)$ število vseh grup reda $\leq n$, katere imajo vse podgrupe edinke. Prvih 200 vrednosti števila $v(n)$ ter števila $w(n)$ je prikazanih v tabelah 6.5 in 6.6.

Tabela 6.5: Začetne vrednosti števila $v(n)$, kjer je $n = 1, 2, ..., 200$.

n	1				5					10
0	0	0	0	0	0	0	0	1	1	1
10	1	1	1	1	1	2	2	2	2	2
20	2	2	2	3	3	3	3	3	3	3
30	3	4	4	4	4	4	4	4	4	5
40	5	5	5	5	5	5	5	6	6	6
50	6	6	6	6	6	7	7	7	7	7
60	7	7	7	8	8	8	8	8	8	8
70	8	10	10	10	10	10	10	10	10	11
80	11	11	11	11	11	11	11	12	12	12
90	12	12	12	12	12	13	13	13	13	13
100	13	13	13	14	14	14	14	14	14	14
110	14	15	15	15	15	15	15	15	15	16
120	16	16	16	16	16	16	16	17	17	17
130	17	17	17	17	17	18	18	18	18	18
140	18	18	18	20	20	20	20	20	20	20
150	20	21	21	21	21	21	21	21	21	22
160	22	22	22	22	22	22	22	23	23	23
170	23	23	23	23	23	24	24	24	24	24
180	24	24	24	25	25	25	25	25	25	25
190	25	26	26	26	26	26	26	26	26	28

Tabela 6.6: Začetne vrednosti števila $w(n)$, kjer je $n = 1, 2, ..., 200$.

n	1				5					10
0	1	2	3	5	6	7	8	12	14	15
10	16	18	19	20	21	27	28	30	31	33
20	34	35	36	40	42	43	46	48	49	50
30	51	59	60	61	62	66	67	68	69	73
40	74	75	76	78	80	81	82	88	90	92
50	93	95	96	99	100	104	105	106	107	109
60	110	111	113	125	126	127	128	130	131	132
70	133	141	142	143	145	147	148	149	150	156
80	161	162	163	165	166	167	168	172	173	175
90	176	178	179	180	181	189	190	192	194	198
100	199	200	201	205	206	207	208	214	215	216
110	217	223	224	225	226	228	230	231	232	236
120	238	239	240	242	245	247	248	264	265	266
130	267	269	270	271	274	278	279	280	281	283
140	284	285	286	298	299	300	302	304	305	307
150	308	312	314	315	316	318	319	320	321	329
160	330	335	336	338	339	340	341	345	347	348
170	350	352	353	354	356	362	363	364	365	369
180	370	371	372	376	377	378	379	381	384	385
190	386	398	399	400	401	405	406	408	409	417

Če sedaj pogledamo zaporedji $\{a(n)\}_{n\in\mathbb{N}}$ in $\{h(n)_{n\in\mathbb{N}}\}$ z obratne perspektive, lahko definiramo dve novi zaporedji. Naj $S_a(n)$ označuje najmanjše število $k \in \mathbb{N}$, za katerega velja, da obstaja natanko n neizomorfnih, abelovih grup reda k. V spodnji tabeli je podanih prvih 60 elementov zaporedja $\{S_a(n)\}_{n\in\mathbb{N}}$. V tem primeru 0 pomeni primer, ko $\{S_a(n)\}$ ne obstaja (n ni produkt particije števil).

Tabela 6.7: Začetne vrednosti števila $S_a(n)$, kjer je $n = 1, 2, ..., 60$.

n	1				5					10
0	1	4	8	36	16	72	32	900	216	144
10	64	1800	0	288	128	44100	0	5400	0	3600
20	864	256	0	88200	1296	0	27000	7200	0	512
30	0	5336100	1728	0	2592	264600	0	0	0	176400
40	0	1024	0	2304	3456	0	0	10672200	7776	32400
50	0	0	0	1323000	5184	2048	0	0	0	4608

Naj $S_h(n)$ označuje najmanjše število $k \in \mathbb{N}$, za katerega obstaja natanko n neizomorfnih hamiltonskih grup reda k. Prvih 30 elementov zaporedja $\{S_h(n)_{n\in\mathbb{N}}\}$ je podanih v naslednji tabeli, kjer 0 pomeni primer, ko n ni produkt particije števil in $\{S_h(n)\}$ ne obstaja.

Tabela 6.8: Začetne vrednosti števila $S_h(n)$, kjer je $n = 1, 2, ..., 30$.

n	1				5					10
0	8	72	216	1800	648	5400	1944	88200	27000	16200
10	5832	264600	0	48600	17496	10672200	0	1323000	0	793800
20	243000	52488	0	32016600	405000	0	9261000	2381400	0	157464

Navedene tabele sem povzela iz [2]. Avtorji tega članka so te tabele neredili s pomočjo računalniških izračunov.

Poglavje 7

Zaključek

V zaključni projektni nalogi smo si najprej obrazložili osnovne algebrske pojme. Kaj v algebri pomeni izraz grupa. Pogledali smo nekatere vrste grup, kot so končne oziroma neskončne, abelove, enostavne in torzijske. Ugotovili smo, da je grupe moč prikazati z grupno oz. Cayleyjevo tabelo, iz katere je moč ugotoviti nekaj uporabnih lastnosti grup. Definirali smo pojem podgrupe. Za lažjo predstavo smo ga tudi obrazložili na primerih. V zaključni nalogi nam je bil zelo zanimiv posebni tip podgrup, in sicer tako imenovane edinke, saj velja, da je grupa dedekindova, če so vse njene podgrupe edinke. V poglavju o edinkah smo definirali pojma center in centrilizator. Za vsako abelovo grupo velja, da ima le podgrupe edinke, torej je vsaka abelova grupa primer dedekindove grupe. Obstajajo pa tudi dedekindove grupe, ki niso abelove. To pomeni, da obstajajo neabelove grupe, katerih vse podgrupe so edinke. Take grupe imenujemo hamiltonske grupe. Te je preučeval matematik Richard Dedekind. Najmanjši primer hamiltonske grupe je odkril matematik William Hamilton, to je grupa kvaternionov. Zato smo si najprej ogledali kvaternione, iz katerih je sestavljena grupa kvaternionov Q_8. Ugotovili smo, da je tako kavternione kot grupo kvaternionov moč zapisati na več načinov. Razlaga vseh dosedajšnjih pojmov je bila potrebna, da smo lahko končno klasificirali hamiltonske grupe, glej izrek 5.6. Nazadnje smo kot zanimivost predstavili še število končnih hamiltonskih grup, glede na dan red oziroma moč grupe. Torej glavni cilj zaključne projektne naloge je bil preučevati hamiltonske grupe.

Literatura

[1] Fraleigh, J. B., A first course in abstract algebra, Kingston, Rhode Island:Pearson Education, Inc., 2003.

[2] Horvat, B., Jaklič, G. in Pisanski, T., On the number of hamiltonian groups, Mathematical Communications, 2005, Vol. 10, N_o 1.

[3] Kutnar, K., Malnič A., Marušič D. in Šparl P., Abstraktna algebra: http://www.scribd.com/doc/22501667/Abstraktna-Algebra-Gradivo-za-Algebra-III (Zadnji dostop 12.8.2010).

[4] Milies, C. P. in Sehgal S. K., An introduction to group rings, Dordrecht, Boston: Kluwer Academic, 2002.

[5] Quaternion: http://mathworld.wolfram.com/Quaternion.html (Zadnji dostop 12.8.2010).

[6] Quaternion group: http://mathworld.wolfram.com/QuaternionGroup.html (Zadnji dostop 12.8.2010).

[7] Vidav, I., Algebra, Ljubljana: DMFA - založništvo, 2003.