Univerzitet u Beogradu

Matematički fakultet

Automorfizmi konačno generisanih Abelovih grupa

Master rad

Student: Milica Stanković

Mentor: dr Žarko Mijajlović

26. jun 2010. godine

Sadržaj

"...What we learn from our whole discussion and what has indeed become a guiding principle in modern matematics is this lesson:

Whenever you have to do with a structure-endowed entity, try to determine its group of automorphisms, the group of those element-wise transformation which leave all structural relations undisturbed. You can expect to gain a deep insight into the constitution of that entity. After that you may start to investigate symmetric configurations of elements, i.e. configurations which are invariant under a certain subgroup of the group of all automorphisms; and it may be advisable, before looking for such configurations, to study the subgroups themselves, e.g. the subgroup of those automorphisms which leave one element fixed, or leave two distinct elements fixed, and investigate what discontinuous or finite subgroups there exist, and so forth...

... Symmetry is a vast subject, significant in art and nature. Mathematics lies at its root, and it would be hard to find a better one on which to demonstrate the working of a mathematical intelect. ..."

Hermann Weyl, citat iz knjige *"Symmetry"*

1 Konačno generisane Abelove grupe

1.1 Osnovne definicije

Definicija 1.1.1 *Za neprazan skup G i binarnu operaciju $\cdot : G \times G \to G$ struktura $(G, \cdot)$ je grupa ako*

$$(\forall\, a, b, c \in G) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$
$$(\exists e \in G)(\forall\, a \in G) \quad a \cdot e = e \cdot a = a$$
$$(\forall\, a \in G)(\exists b \in G) \quad a \cdot b = b \cdot a = e$$

Pritom, ako je još i $(\forall\, a, b \in G)\ a \cdot b = b \cdot a$ grupa je Abelova. Običaj je da se kod Abelovih grupa koristi aditivna notacija, tj operacija se označava $+$, neutral sa 0, inverz elementa a sa $-a$. Broj elemenata skupa G naziva se red grupe, u oznaci $|G|$.

Za proizvoljan element $a \in G$ skup elemenata oblika $ka, k \in \mathbb{Z}$ označavamo $< a >$. Jasno je da je to podgrupa grupe G. U slučaju da među elementima ka nema jednakih, ona je beskonačna. U drugom slučaju neka postoje jednaki elementi $ka = ma$ i neka je $k > m$. Tada je $(k - m)a = 0$. Pritom postoji i najmanji n za koji je $na = 0$.

Definicija 1.1.2 *Grupa se naziva ciklična ako je generisana jednim elementom, odnosno, za neko a, $G =< a >= \{ka : k \in \mathbb{Z}\}$. Ako je ciklična grupa konačna, njen red je najmanji broj n za koji $na = 0$. Broj n je red elementa $a \in G$. Za elemente koji nisu konačnog reda kažemo da su beskonačnog reda.*

Teorema 1.1.3 *Svaka ciklična grupa je izomorfna sa $\mathbb{Z}_n$ ako je konačnog reda ili sa $\mathbb{Z}$ ako je beskonačnog reda.*

Dokaz: Neka je $G =< a >$, $red(a) = n$. Proizvoljan $m \in \mathbb{Z}$ može se predstaviti $m = kn + r$, zato $ma = (nk + r)a = 0 + ra = ra$, pritom je $r < n$. Dakle $G = \{0, a, 2a, ...(n-1)a\}$ i među njima nema jednakih. Uočimo preslikavanje $f : G \to \mathbb{Z}_n$ tako da $f(ra) = r$. Preslikavanje je dobro definisano, "na" i "1-1". Takođe $f(r_1a + r_2a) = f((r_1 + r_2)a) = r_1 + r_2 = f(r_1a) + f(r_2a)$. Dakle, f je izomorfizam. Neka je sada $G =< a >$ beskonačnog reda. Tada među elementima ka nema jednakih, jer ako pretpostavimo suprotno $ka = ma$, tada postoji broj $k-m$ za koji je $(k-m)a = 0$, pa je red G konačan. Preslikavanje $f : G \to \mathbb{Z}$ je izomorfizam. $\Diamond$

Dakle, jedine ciklične grupe označavaćemo $\mathbb{C}_n$ odnosno $\mathbb{C}_\infty$.

Teorema 1.1.4 $\mathbb{C}_n \times \mathbb{C}_m \cong \mathbb{C}_{nm}$ *akko* $(n, m) = 1$

Dokaz: Neka su generatori $\mathbb{C}_n$,$\mathbb{C}_m$ i $\mathbb{C}_{mn}$ redom a, b i c.
$\Rightarrow$ Pretpostavimo da $(n, m) = d \neq 1$ i neka $k = NZS(m, n) = \frac{mn}{d}$. Neka je (pa, qb) proizvoljan element $\mathbb{C}_n \times \mathbb{C}_m$. Primetimo da je $k(pa, qb) = (kpa, kpb) = (\frac{mn}{d}pa, \frac{mn}{d}qb) = (\frac{mp}{d}na, \frac{nq}{d}ma) = (e, e)$. Zaključujemo, svaki element iz $\mathbb{C}_n \times \mathbb{C}_m$ je reda strogo manjeg od mn, dakle $\mathbb{C}_n \times \mathbb{C}_m \ncong \mathbb{C}_{nm}$
$\Leftarrow$ Uočimo preslikavanje $f : \mathbb{C}_n \times \mathbb{C}_m \to \mathbb{C}_{nm}$ definisano na sledeći način: $f((a, e)) = nc, f((e, b)) = mc$ i $f((pa, qb)) = pf(a, e) + qf(e, b)$. Dokaže se lako da je to izomorfizam. $\Diamond$

Definicija 1.1.5 *Neka je $(G, +)$ proizvoljna grupa. Preslikavanje $f : G \to G$ tako da*

$$(\forall\, a, b \in G) \quad \mathrm{f}(a + b) = \mathrm{f}(a) + \mathrm{f}(b)$$

je endomorfizam. Bijektivni endomorfizmi nazivaju se automorfizmi grupe G.

Ako uočimo $EndG$ skup svih endomorfizama proizvoljne grupe G i operacije $+ : (f+g)(x) = f(x) + g(x)$ i $\circ$ kompozicija, za proizvoljna dva endomorfizma važi

$$(f+g)(a+b) = f(a+b) + g(a+b) = f(a) + f(b) + g(a) + g(b)$$

pa o tome da $f+g \in EndG$ možemo zaključiti jedino ako je G komutativna. Dakle, za komutativnu grupu G, $(EndG\,, +)$ je grupa. Zatim, za proizvoljan endomorfizam f inverz za operaciju $\circ$ u opštem slučaju ne mora da postoji u $EndG$, dok se ostale osobine prstena lako pokazuju. Označimo u $EndG$ neutral za sabiranje $\mathbf{0}$. Svi automorfizmi su invertibilni u odnosu na $\circ$, pa možemo reći $AutG = EndG^* = EndG\backslash\{\mathbf{0}\}$.

Time je dokazano tvrđenje

Teorema 1.1.6 *Ako je* G *Abelova grupa,* $(EndG\,, +, \circ)$ *je prsten,* $(AutG\,, \circ)$ *je grupa.* $\Diamond$

1.2 Slobodne Abelove grupe

Uočimo proizvoljan element a iz komutativne grupe G. Možemo uočiti preslikavanje $\mathbb{Z} \times G \to G$

$$(n, a) \to na = \underbrace{a + a + \ldots + a}_{n}$$

Tako operacija iz grupe G indukuje spoljnu $\mathbb{Z}$ - operaciju u grupi G. Primećujemo da važe aksiome modula:

$$\begin{aligned}
&(G\,, +) \textit{ je komutativna grupa}\\
&\alpha(a+b) = \alpha a + \alpha b\\
&(\alpha+\beta)a = \alpha a + \beta a\\
&\alpha(\beta a) = (\alpha\beta)a\\
&1a = a
\end{aligned}$$

Biće značajno da posmatramo strukturu $(G, +, \cdot)$ koju ćemo nazivati modul nad prstenom $\mathbb{Z}$ odnosno $\mathbb{Z}$ - modul (moduli nad poljem umesto prstena su dobro poznati vektorski prostori). Sada možemo određene elemente komutativne grupe G da posmatramo kao bazu, a ostale kao linearne kombinacije ovih, i slične mogućnosti koje bi pružao vektorski prostor.

Definicija 1.2.1 *Neka je* $(G, +)$ *komutativna grupa a time i* $\mathbb{Z}$ *- modul. Element* $a \in G$ *naziva se linearna kombinacija elemenata* $e_1, e_2, \ldots, e_n \in G$ *ako je* $a = \sum_i a_i e_i$ *gde su* $a_i \in \mathbb{Z}$, $i \in \{1, \ldots, n\}$. *Skup svih linearnih kombinacija elemenata* $e_1, e_2, \ldots, e_n \in G$ *naziva se linearni omotač* $\mathcal{L}\{e_1, \ldots, e_n\}$. *Ukoliko je* $\mathcal{L}\{e_1, \ldots, e_n\} = G$, G *je generisana elementima* e_i.

Neka je preslikavanje $L : \mathbb{Z}^n \to G$ definisano

$$L(a_1, \ldots, a_n) = a_1 e_1 + \ldots + a_n e_n$$

To je homomorfizam modula $\mathbb{Z}^n$ u modul G. Grupa G je konačno generisana elementima e_i ako i samo ako L je epimorfizam. Dalje, L je monomorfizam akko mu je jezgro trivijalno, odnosno $a_1 e_1 + \ldots + a_n e_n = 0 \;\Rightarrow a_1 = \ldots = a_n = 0$

Definicija 1.2.2 *Skup elemenata* $e_1, e_2, \ldots, e_n \in G$ *je linearno nezavisan ako* $a_1 e_1 + \ldots + a_n e_n = 0 \;\Rightarrow a_1 = \ldots = a_n = 0$, *u suprotnom, taj sistem vektora je linearno zavisan.*

Definicija 1.2.3 *Komutativna grupa se naziva slobodna ako ima linearno nezavisnu generatrisu.*

Teorema 1.2.4 *Slobodna Abelova grupa* G *je obavezno* $\mathbb{Z}^n$.

Dokaz: Jasno, $\mathbb{Z}^n$ je slobodna, njena konačna linearno nezavisna generatrisa je $(1,0,\ldots,0),\ldots,(0,0,\ldots,1)$. Neka komutativna grupa G ima konačnu linearno nezavisnu generatrisu e_1, $e_2,\ldots,$ $e_n \in G$, dakle svaki element se može predstaviti $a = a_1e_1 + \ldots + a_ne_n$, $a_i \in \mathbb{Z}$ a sama grupa $G = e_1\mathbb{Z} \times \ldots \times e_n\mathbb{Z}$. Iz činjenice da su e_i linearno nezavisni, tj $a_1e_1 + \ldots + a_ne_n = 0 \Rightarrow a_1 = \ldots = a_n = 0$ sledi $e_i\mathbb{Z} \cong \mathbb{Z}$ jer, druga mogućnost je da bude $e_i\mathbb{Z} \cong \mathbb{C}_m$ ali tada bi postojao broj $k : ke_i = 0$ što je u suprotnosti sa pretpostavkom o linearnoj nezavisnosti. Dakle, slobodne Abelove grupe sa konačnom bazom su $\mathbb{Z}^n$ $\Diamond$

Posledica 1.2.5 *Ako je G slobodna Abelova grupa generisana sa $e_1,\ldots e_n$ onda je $G =< e_1 > \oplus \ldots \oplus < e_n >$* $\Diamond$

Primedba: *Pojam slobodne Abelove grupe G može se definisati i kao grupa sa određenom generatrisom X iz koje se svaki homomorfizam iz X u Abelovu grupu H diže na celu grupu G. Ovde je to tvrđenje.*

Teorema 1.2.6 *Neka je G slobodna Abelova grupa i A i B njene podgrupe tako da je $G = A \oplus B$. Neka je H proizvoljna grupa i homomorfizmi $\phi : A \to H$ i $\psi : B \to H$. Tada postoji $\theta : G \to H$ homomorfizam koji se na A poklapa sa ϕ, a na B sa ψ*

Dokaz: Jasno, pošto se svaki element $g \in G$ jedinstveno predstavlja kao $g = a + b$, traženi homomorfizam je $\theta(a + b) = \phi(a) + \psi(b)$. $\Diamond$

Teorema 1.2.7 *Svaka Abelova grupa* G *je homomorfna slika neke slobodne Abelove grupe* H.

Dokaz: Neka je $H = \mathbb{Z}^n$ slobodna Abelova grupa sa bazom e_1, $e_2,\ldots,$ e_n. Uočimo pomenuto preslikavanje $L : H \to G$, $L(a_1 \ldots a_n) = a_1c_1 + \ldots + a_nc_n \in G$. Svaki element iz H se jedinstveno predstavlja kao $a_1e_1 + \ldots + a_ne_n$, pa je to traženi homomorfizam. $\Diamond$

Posledica 1.2.8 *Svaka konačno generisana grupa je izomorfna količniku slobodne grupe i njene podgrupe.*

Dokaz: Neka je G generisana sa c_1, $c_2,\ldots,$ c_n. Uočimo homomorfizam iz prethodne teoreme, $ImL = G$ i tvrđenje sledi iz $H/KerL \cong ImL$ $\Diamond$

Teorema 1.2.9 *Ako slobodna Abelova grupa ima bar jednu konačnu generatrisu onda su sve njene baze konačne i sa istim brojem elemenata.*

Dokaz: Neka je $\overline{e}$ neka baza i $f_1,\ldots,f_m$ konačna generatrisa, tada je svaki f_i kombinacija konačno mnogo elemenata iz $\overline{e}$. Neka su ti elementi $e_1,\ldots,e_n$, njihov linearni omotač sadrži linearni omotač sistema f_i, a to je cela grupa. Pošto su elementi iz $\overline{e}$ linearno nezavisni i $e_1,\ldots,e_n \subset \overline{e}$, znači da je $e_1,\ldots,e_n = \overline{e}$. Za drugi deo tvrđenja, neka su e, f dve baze sa n, m elemenata respektivno. Postoje matrice P, formata (n,m) i Q, formata (m,n), za koje $f = eP, e = fQ$. Odavde

$$\begin{aligned} e &= eE_n = fQ = ePQ \\ f &= fE_m = eP = fQp \\ &\Rightarrow E_n = PQ, E_m = QP \end{aligned}$$

Pošto je $TrPQ = TrQP$, vidimo da je $TrE_n = TrE_m$, odnosno $m = n$. $\Diamond$

Sada je korektno definisati *rang* slobodne Abelove grupe.

Definicija 1.2.10 *Neka je G slobodna Abelova grupa sa konačnom bazom. Broj elemenata u bazi naziva se rang grupe G.*

1.3 Teorema o razlaganju konačno generisanih Abelovih grupa

Teorema 1.3.1 *Za svaku matricu $A \in M_{mn}(\mathbb{Z})$ postoje invertibilne matrice P i Q i matrica $A^0 = PAQ$ čiji elementi na dijagonali su jedinstveno određeni do na znak, oblika*

$$A^0 = \begin{pmatrix} n_1 & \dots & 0 & \dots & 0 \\ \vdots & & & & \\ 0 & \dots & n_k & \dots & 0 \\ \vdots & & & & \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix} \quad (n_i | n_{i+1})$$

Dokaz: Treba dokazati da se primenom konačno mnogo elementarnih transformacija kolona i vrsta od matrice A može dobiti matrica traženog oblika. Pritom vodimo računa o tome da u $\mathbb{Z}$ jedino $-1, 1$ imaju inverz. Primeniti elementarnu transformaciju kolona odnosno vrsta ϕ na matricu A znači $\phi(A) = A\phi(E)$, odnosno $\phi(A) = \phi(E)A$. Konačni proizvodi ovih invertibilnih matrica daju matrice P i Q. Najpre ćemo dokazati da se A može svesti na oblik

$$\begin{pmatrix} d & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2n} \\ \vdots & & & \\ 0 & b_{m2} & \dots & b_{mn} \end{pmatrix} \quad (d | b_{ij})$$

Neka je p najmanji od apsolutnih vrednosti elemenata matrice koji nisu 0, $p = min|a_{ij}|$. Dokaz ćemo izvesti indukcijom po broju p. Zamenom mesta vrsta i kolona možemo dovesti da p bude na mestu a_{11}. Ako je $p = 1$ pomnožimo sa $-a_{i1}$ i dodamo i - toj vrsti, i analogno pomnožimo sa $-a_{1i}$ pa dodamo i - toj koloni, i tu smo dobili traženi oblik jer $1|a \in \mathbb{Z}$. Ako je $p \neq 1$, pretpostavimo da možemo dobiti traženi oblik za sve matrice C za koje je $min(c_{ij}) < p$. Podelimo a_{21} sa a_{11}, $a_{21} = a_{11}q_{21} + r_{21}$, gde je $r_{21} \leq a_{11}$ i analogno sve ostale elemente prve vrste i prve kolone. Matrica A se može napisati kao

$$\begin{pmatrix} a_{11} & a_{11}q_{12} + r_{12} & \dots & a_{1n} + r_{1n} \\ a_{11}q_{21} + r_{21} & a_{22} & \dots & a_{2n} \\ \vdots & & & \\ a_{11}q_{n1} + r_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & b_{22} & \dots & b_{2n} \\ \vdots & & & \\ r_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}$$

Kada pomnožimo sa odgovarajućim q i dodamo odgovarajućim vrstama i kolonama, ostaje ili matrica traženog oblika, ili matrica sa r - ovima koji su manji od p, tu $a_{11} = d$, a ako i ne deli neki od b_{ij} - ova, može se dovesti do traženog oblika.

I opet indukcijom po broju vrsta ili kolona. $\Diamond$

Teorema 1.3.2 *Neka je G slobodna Abelova grupa ranga n. Za svaku pravu podgrupu H, postoji sistem celih brojeva $n_1, \dots, n_k$, $n_i | n_{i+1}$ određenih jednoznačno do na znak, za koje G ima bazu $e_1, \dots, e_n$, a baza za H je $n_1e_1, \dots, n_ke_k$*

Dokaz: H je takođe slobodna. Neka su g i h baze za G i H. Tada je $h = gA$ za neku matricu nad $\mathbb{Z}$. Prema prethodnom tvrđenju postoji matrica $A^0 = PAQ$ i lako vidimo da je $f = eA^0$. $\Diamond$

Teorema 1.3.3 *Neka je $G = A \oplus B$ i neka su $A_1 \leq A, B_1 \leq B, N = A_1 + B_1$. Tada $G/N = A/A_1 \oplus B/B_1$*

Dokaz: Neka su $\phi : A \to A/A_1$ i $\psi : B \to B/B_1$ prirodni epimorfizmi. Oni se mogu proširiti do homomorfizma $\theta : G \to A/A_1 \oplus B/B_1$. Nađimo jezgro: ono sadrži jezgra od ϕ, ψ, odnosno $A_1 + B_1 \subseteq Ker\theta$. S druge strane, ako x pripada $Ker\theta \subseteq G$ može sa jedinstveno predstaviti $x = a + b$ za neke $a \in A, b \in B$. $\theta(x) = \phi(a) + \psi(b) = 0$ povlači $a \in Ker\phi = A_1, b \in Ker\psi = B_1$, zato $A_1 + B_1 = Ker\theta$ $\Diamond$

Sada možemo dokazati teoremu o razlaganju.

Teorema 1.3.4 *Svaka konačno generisana Abelova grupa je proizvod cikličnih grupa.*

Dokaz: Svaka Abelova grupa generisana sa n elemenata e_i je količnik slobodne grupe $\mathbb{Z}^n$ po podgrupi H koja je takođe slobodna i ranga $k \leq n$. Ali, za svaku podgrupu slobodne grupe postoji sistem brojeva $n_1, \ldots, n_k$ od kojih svaki deli sledeći za koje je $< n_1 e_1, \ldots, n_k e_k >= H$, a prethodno tvrđenje opravdava sečenje $G = \mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z} \oplus \mathbb{Z}^s$. $\Diamond$

2 Automorfizmi konačno generisanih Abelovih grupa

Svaka konačno generisana Abelova grupa može se predstaviti kao proizvod cikličnih grupa pa njenu strukturu možemo izučiti pomoću jednostavnijih cikličnih grupa. Tako očekujemo da se neka pravilnost ispolji i kod njenih automorfizama. Već je dobro poznata činjenica da automorfizmi čine grupu u odnosu na kompoziciju, ali ona nije uvek Abelova. Ovde će biti opisana struktura grupe automorfizama konačno generisanih Abelovih grupa.

2.1 Ojlerova grupa Φ_n

Najpre ćemo navesti poznata tvrđenja o $\mathbb{C}_n$.

Lema 2.1.1 *Neka je* $\mathbb{C}_n =< a >$. *Tada za svako* $k \in \mathbb{Z} < a^k >=< a^{NZD(n,k)} >$, *i red elementa* a^k *je* $\frac{n}{NZD(n,k)}$.

Dokaz: Neka je $k < n, d = NZD(n,k)$. Prvo, $(a^k)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = 1$, a kad bi postojao manji $k_1|\frac{n}{d}, (a^k)^{k_1} = 1$, pa $n|k_1k$. Neka je a^l proizvoljan element od $< a^k >$, odnosno, $a^l = a^{l_1k} = a^{l_1k_1d} = (a^d)^{l_1k_1}$. Dakle, a^d je generator od $< a^k >$. $\Diamond$

Definicija 2.1.2 *Grupa invertibilnih elemenata* $\mathbb{Z}_n^* = \Phi_n$ *naziva se Ojlerova grupa. Njen red je* $\phi(n)$ *Ojlerova funkcija.*

Teorema 2.1.3 $Aut(Z)_n \cong \Phi_n$

Dokaz: Svaki automorfizam čuva red elementa, i slika generatore u generatore. Ako je $(Z)_n =< a >$, opcije za sliku ovog generatora su upravo elementi reda istog kao a. To su elementi uzajamno prosti sa n. Za proizvoljni automorfizam ϕ uočimo preslikavanje $f : \phi \to k$, gde $\phi(a) = k$ i to je traženi izomorfizam. $\Diamond$

2.2 Linearna grupa $Gl_n(\mathbb{F}_p)$

Definicija 2.2.1 *Neka je* $\mathbb{F}$ *proizvoljno polje. Skup invertibilnih matrica formata* $n \times n$ *sa elementima iz polja* $\mathbb{F}$ *naziva se opšta linearna grupa stepena* n *u oznaci* $GL_n(\mathbb{F})$.

Neka je V vektorski prostor konačne dimenzije n nad poljem $\mathbb{F}$. Odaberimo jednu fiksiranu bazu. Svaki automorfizam $\phi : V \to V$ je jedinstveno određen slikama elemenata iz baze, i može se predstaviti jedinstvenom matricom iz $M_n(\mathbb{F})$ čije kolone predstavljaju slike baznih vektora. Pošto automorfizmi slikaju baze u baze, slike baznih vektora moraju biti linearno nezavisne, odnosno, matrica preslikavanja ima determinantu različitu od nule.

Teorema 2.2.2 *Za vektorski prostor* V *konačne dimenzije* n *nad poljem* $\mathbb{F}$ *važi* $Aut(V) \cong GL_n(\mathbb{F})$.

Dokaz: Neka je $e_1, \ldots, e_n$ baza i $v = \sum_{1 \le i \le n} v_i e_i \in V$. Preslikavanje $f : AutV \to GL_n(\mathbb{F})$ definisano $f(\phi) = A$ za koje $\phi(v) = A \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ je traženi izomorfizam. $\Diamond$

Napomena: *Za vektorske prostore beskonačne dimenzije definiše se upravo* $GL(V) = Aut(V)$.

Posledica 2.2.3 $Aut(\mathbb{Z}_p^n) \cong GL_n(\mathbb{F}_p)$

Dokaz: Abelova grupa $\mathbb{Z}_p^n$ predstavlja modul nad $\mathbb{Z}_p$ ali to je upravo polje $\mathbb{Z}_p = \mathbb{F}_p$, pa je ta grupa vektorski prostor dimenzije n nad poljem $\mathbb{F}$ i dokaz sledi iz prethodnog tvrđenja. $\Diamond$

Sada vidimo šta je grupa automorfizama konačnog proizvoda $\mathbb{Z}_p^n$. U sledećem odeljku biće pokazan opštiji rezultat iz koga će slediti ovaj zaključak, ali je ovo razmatranje bilo pogodno da objasni motivaciju i slične principe za dalje.

2.3 Automorfizmi konačnih Abelovih grupa

Sledeće važi za sve konačne grupe uzajamno prostih redova, ne mora obavezno komutativne. Sve operacije će biti označene multiplikativno, imajući u vidu da se u svakom trenutku radi o odgovarajućoj operaciji grupe iz koje su elementi.

Lema 2.3.1 *Neka su H i G konačne grupe uzajammno prostih redova, prirodne projekcije $\pi_G : G \times H \to G$ i $\pi_H : G \times H \to H$ i $\omega \in Aut(G \times H)$. Tada su trivijalna preslikavanja*

$$\alpha : G \to H,\ \alpha(g) = \pi_H(\omega(g, 1_H))$$
$$\beta : H \to G,\ \beta(h) = \pi_G(\omega(1_G, h))$$

Dokaz: Preslikavanje α je homomorfizam:

$$\alpha(g_1g_2) = \pi_H(\omega(g_1g_2, 1_H)) = \pi_H(\omega(g_1, 1_H)(\omega(g_2, 1_H)) = \pi_H(\omega(g_1, 1_H))\pi_H(\omega(g_2, 1_H)) = \alpha(g_1)\alpha(g_2)$$

Neka su $n = |G|, m = |H|$. Nađimo jezgro $Ker\alpha$:

$$\alpha(g^m) = \pi_H(\omega(g^m, 1_H)) = \pi_H(\omega(g, 1_H)^m) = \pi_H(g_1, h^m) = 1_H,\ g \in G$$

Zato $\{g^m : g \in G\} \subseteq Ker\alpha \subseteq G$. Pošto su $(m, n) = 1$ ovaj skup ima tačno n elemenata, dakle $Ker\alpha = G$, odnosno, preslikavanje je trivijalno. Analogno za preslikavanje β. $\Diamond$

Teorema 2.3.2 *Neka su H i G konačne grupe uzajammno prostih redova. Tada je $Aut(G \times H) \cong AutG \times AutH$*

Dokaz: Uočimo preslikavanje $\phi : AutG \times AutH \to Aut(G \times H), \phi(\alpha, \beta)(g, h) = (\alpha(g), \beta(h))$.
ϕ je xomomorfizam:

$$\phi((\alpha_1, \beta_1)(\alpha_2, \beta_2))(g, h) = \phi((\alpha_1\alpha_2)(g), (\beta_1\beta_2)(h)) = \phi(\alpha_1, \beta_1)\phi(\alpha_2, \beta_2)(g, h)$$

ϕ je "1-1":

$$\phi(\alpha_1, \beta_1) = \phi(\alpha_2, \beta_2) \Rightarrow$$
$$(\alpha_1(g), \beta_1(h)) = (\alpha_2(g), \beta_2(h)) \Rightarrow$$
$$\alpha_1(g) = \alpha_2(g), \beta_1(h) = \beta_2(h) \Rightarrow$$
$$(\alpha_1, \beta_1) = (\alpha_2, \beta_2)$$

ϕ je "na": Za proizvoljan $\omega \in Aut(G \times H)$ treba pronaći $\omega_G \in AutG$ i $\omega_H \in AutH$ tako da je $\phi(\omega_G, \omega_H) = \omega$.
Neka su $\omega_G(g) = \pi_G(\omega(g, 1_H))$ i $\omega_H(h) = \pi_H(\omega(1_G, h))$. Iz prethodne leme zaključujemo da su ova preslikavanja dobro definisana i da su to endomorfizmi G odnosno H. Važi

$$\omega(g, h) = \omega(g, 1_H)\omega(1_G, h) = (\omega_G(g), \omega_H(h))$$

Dakle $\phi(\omega_G, \omega_H) = \omega$. Grupe G i H su konačne, zato je dovoljno pokazati da su to monomorfizmi. Neka je $g \in Ker\omega_G$. Tada

$$\omega(g, 1_H) = (\omega_G(g), \omega_H(1_H)) = (1_G, 1_H)$$

a ω je automorfizam pa je dokaz završen. $\Diamond$

Prethodno tvrđenje posebno važi za konačne Abelove grupe, pa je u tom slučaju grupa automorfizama proizvod $AutH_p$ po prostim brojevima koji dele red te grupe. Sada će biti opisana grupa $AutH_p$, gde je

$$H_p = \mathbb{Z}_{p^{e_1}} \times \ldots \times \mathbb{Z}_{p^{e_n}},\ p \in Prost,\ 1 \leq e_1 \leq \ldots \leq e_n$$

Svako linearno preslikavanje (homomorfizam) vektorskih prostora možemo prikazati odgovarajućom matricom čije kolone su koordinate slika baznih vektora pri tom preslikavanju. Preciznije za vektorski prostor V nad K konačne dimenzije n, svaki endomorfizam zavisi od odabrane baze vektorskog prostora. U prethodnom odeljku pokazali smo $Aut(V) \cong GL_n(\mathbb{K})$. Očekujemo slične osobine i kod modula H_p nad prstenom $\mathbb{Z}$. Ali, zbog činjenice da u $\mathbb{Z}$ samo $-1, 1$ imaju inverz za množenje, u skupu $M_n(\mathbb{Z})$ za elementarne transformacije neophodno je da odgovarajući elementi kao činioce imaju stepene od p koji učestvuju kao redovi elemenata H_p. Biće uočen skup matrica R_p koji je prsten u odnosu na množenje matrica, epimorfizam tog prstena na $EndH_p$, a zatim identifikovani invertibilni elementi $AutH_p$. Ovo je pristup koji su preporučili *C. Hillar* i *D. Rhea* [1].

Uočimo da se svaki element iz H_p predstavlja $x = g_1r_1 + \dots g_nr_n$. Svaki automorfizam je dovoljno definisati na generatorima, pa neka su $r_1^*, \dots, r_n^*$ slike ovih generatora pri nekom automorfizmu. Preciznije:

$$\begin{pmatrix} r_1^* \\ \vdots \\ r_n^* \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$$

Važi $p^{e_i}r_i^* = 0$, jer se čuva red elemenata, pa je

$$p^{e_i}r_i^* = p^{e_i}(a_{i1}r_1 + \dots + a_{in}r_n) = 0$$

a r_j linearno nezavisni, pa za svako i, $p^{e_i}a_{ij} = 0\,(mod\, p^{e_j})$, odnosno $p^{e_j}|p^{e_i}a_{ij}$. Sada za $i \leq j$, $p^{e_j-e_i}|a_{ij}$.

Definicija 2.3.3

$$R_p = \{A = (a_{ij}) \in M_n(\mathbb{Z}) : p^{e_j-e_i}|a_{ij}, i \leq j\}$$

Razmotrimo šta znači ovaj uslov. Neka je

$$P = \begin{pmatrix} p^{e_1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & p^{e_n} \end{pmatrix} P^{-1} = \begin{pmatrix} p^{-e_1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & p^{-e_n} \end{pmatrix}, P^{-1} \in M_n(\mathbb{Q})$$

Neka je $A \in R_p$. Važi: $PAP^{-1} =$

$$\begin{pmatrix} b_{11}p^{e_1} & b_{12}p^{e_1} & \dots & b_{1n}p^{e_1} \\ b_{21}p^{e_2} & b_{22}p^{e_2} & \dots & b_{2n}p^{e_2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1}p^{e_n} & b_{n2}p^{e_n} & \dots & b_{nn}p^{e_n} \end{pmatrix} \begin{pmatrix} p^{-e_1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & p^{-e_n} \end{pmatrix} =$$

$$\begin{pmatrix} b_{11} & b_{12}p^{-e_2+e_1} & \dots & b_{1n}p^{-e_n+e_1} \\ b_{21}p^{e_2-e_1} & b_{22} & \dots & b_{2n}p^{-e_n+e_2} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1}p^{e_n-e_1} & b_{n2}p^{e_n-e_2} & \dots & b_{nn} \end{pmatrix}$$

Rezultat je jasno matrica sa racionalnim elementima. Ali pošto je $A \in R_p$ to znači da $p^{e_j-e_i}|b_{ij}, 1 \leq i \leq j \leq n$ a to upravo znači da elementi iznad glavne dijagonale ove matrice pripadaju $\mathbb{Z}$. Zato možemo reći da je $A \in R_p$ ekvivalentno postoji matrica celih brojeva $A_1 \in M_n(\mathbb{Z})$ za koju je $A = P^{-1}A_1P$

Lema 2.3.4 $(R_p, +, \cdot)$ *je prsten.*

Dokaz: Neka su $A, B \in R_p$. $A + B \in R_p$, jer ako $p^{e_j - e_i} | a_{ij}$ i $p^{e_j - e_i} | b_{ij}$, onda i $p^{e_j - e_i} | a_{ij} + b_{ij}$. Inverz za A takođe pripada R_p, jer ako $p^{e_j - e_i} | a_{ij}$ onda i $p^{e_j - e_i} | - a_{ij}$

Neka su $A, B \in R_p$. To znači da postoje matrice celih brojeva A_1, B_1 za koje je $A = P^{-1}A_1P, B = P^{-1}B_1P$. Zato $AB = P^{-1}A_1PP^{-1}B_1P = P^{-1}A_1B_1P$ a to znači da i $AB \in R_p$. Množenje matrica je asocijativno, distributivno u odnosu na sabiranje, i jedinična matrica pripada R_p. Time je dokaz završen. $\Diamond$

Setimo se homomorfizma iz prethodnog odeljka $L : \mathbb{Z}^n \to H_p, L(a_1, \ldots, a_n)^T = (h_1, \ldots, h_n)$. (Radi umanjenja mogućnosti zabune zapišimo elemente iz $\mathbb{Z}^n$ u kolone a elemente iz H_p u vrste.)

Teorema 2.3.5 *Preslikavanje $\phi : R_p \to EndH_p$ definisano $\phi(A) = \phi_A$ za koje $\phi_A(h_1, \ldots, h_n) = L(A^T(h_1, \ldots, h_n))$ je epimorfizam prstena.*

Dokaz: ϕ_A je dobro definisano:
Moramo proveriti da je $L(A^T(h_1, \ldots, h_n)) \in H_p$ dobro definisano.

$L(A^T(h_1, \ldots, h_n)) =$

$$L\Big(\begin{pmatrix} a_{11} & \ldots & a_{n1} \\ \vdots & & \vdots \\ a_{1n} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}\Big) = L\Big(\begin{pmatrix} a_{11}h_1 + \ldots + a_{n1}h_n \\ \vdots \\ a_{1n}h_1 + \ldots + a_{nn}h_n \end{pmatrix}\Big)$$

Elementi u ovoj koloni su neki celi brojevi. Neka su $(h_1, \ldots, h_n) = (g_1, \ldots, g_n)$. Uočimo

$$L\Big(\begin{pmatrix} a_{11}h_1 + \ldots + a_{n1}h_n \\ \vdots \\ a_{1n}h_1 + \ldots + a_{nn}h_n \end{pmatrix}\Big) - L\Big(\begin{pmatrix} a_{11}g_1 + \ldots + a_{n1}g_n \\ \vdots \\ a_{1n}g_1 + \ldots + a_{nn}g_n \end{pmatrix}\Big) =$$

$$L\Big(\begin{pmatrix} a_{11}(h_1 - g_1) + \ldots + a_{n1}(h_n - g_n) \\ \vdots \\ a_{1n}(h_1 - g_1) + \ldots + a_{nn}(h_n - g_n) \end{pmatrix}\Big)$$

Sliku k - te vrste označimo $L_k(a_{1k}(h_1 - g_1) + \ldots + a_{nk}(h_n - g_n))$. Treba to da bude nula u $\mathbb{Z}_{p^{e_k}}$ za svako k. Pošto je $A \in R_p$, važi
$L_k(a_{1k}(h_1 - g_1) + \ldots + a_{nk}(h_n - g_n)) =$
$L_k(a_{1k}(h_1 - g_1)\frac{p^{e_k - e_1}}{p^{e_k - e_1}} + \ldots + a_{(k-1)k}(h_{k-1} - g_{k-1})\frac{p^{e_k - e_{k-1}}}{p^{e_k - e_{k-1}}} + a_{kk}(h_k - g_k) + \ldots + a_{nk}(h_n - g_n))$, pa za $k \geq i$, $p^k | p^{e_k - e_i}$, a za $k < i$, $p^k | (h_i - g_i)$. ϕ_A je linearno kao kompozicija dva linearna preslikavanja, dakle $\phi_A \in EndH_p$.
ϕ je epimorfizam:
Neka je $v_i = (0, \ldots, g_i, \ldots, 0)$. Svaki endomorfizam $M \in EndH_p$ je jedinstveno određen na generatorima v_i, i neka su $M(v_i) = (h_{i1}, \ldots, h_{in})$. Vazi

$$0 = M(0) = M(p^{e_i}v_i) = \underbrace{M(v_i) + \ldots + M(v_i)}_{p^{e_i}} = (p^{e_i}h_{i1}, \ldots, p^{e_i}h_{in})$$

Odavde sledi da $p^{e_j} | p^{e_i}h_{ij}$ odnosno $p^{e_j - e_i} | h_{ij}, i \leq j$. Za matricu $H = (h_{ij})$ važi $\phi(H) = M$. $\Diamond$

Teorema 2.3.6 *Jezgro epimorfizma ϕ je skup matrica $A = (a_{ij})$ takvih da $p^{e_j} | a_{ij}$, za sve i, j.*

Dokaz: Neka je A matrica u kojoj važi uslov teoreme. Tada uočimo slike vrsta kao u prethodnom tvrđenju: $L_k(a_{1k}h_1 + \ldots + a_{nk}h_n) = 0$ u $\mathbb{Z}_{p^{e_k}}$ pošto $p^{e_k} | a_{kj}$, za sve j. Dakle $\phi(A) = 0$. Obrnuto, neka je $\phi(A) = 0$, i $h_1, \ldots, h_n$ koordinate od $x \in H_p$

$$L\Big(\begin{pmatrix} a_{11} & \ldots & a_{n1} \\ \vdots & & \vdots \\ a_{1n} & \ldots & a_{nn} \end{pmatrix} \begin{pmatrix} h_1 \\ \vdots \\ h_n \end{pmatrix}\Big) = 0$$

To znači da su svi $L_j(a_{1j}h_1 + \ldots + a_{nj}h_n) = 0$, odnosno
$L_j(a_{1j}h_1 + \ldots + a_{nj}h_n) = p^{e_j}q$, a to znači da obavezno mora $p^{e_j} | a_{ij}$. $\Diamond$

Prema teoremi o izomorfizmu prstena $R_p/Ker\phi \cong EndH_p$. Tako vidimo kakve matrice iz R_p odgovaraju kojim endomorfizmima H_p. Ovo razmatranje je posebno pogodno za identifikovanje invertibilnih elemenata u $R_p/Ker\phi$, koji predstavljaju automorfizme H_p. Pre toga je potrebna jedna lema.

Lema 2.3.7 *Za svaku matricu $A \in M_n(\mathbb{Z}), det(A) \neq 0$ postoji jedinstvena matrica $B \in M_n(\mathbb{Z})$ za koju $AB = BA = det(A)I$, takozvana* adjungovana matrica. *Ako je $A \in R_p$, onda i $B \in R_P$.*

Dokaz: Za dokaz drugog dela leme neka je $A = P^{-1}A_1P, A_1 \in M_n\mathbb{Z}$ i neka je $B_1 \in M_n\mathbb{Z}$ tako da je $A_1B_1 = B_1A_1 = det(A_1)I = det(A)I$. Stavimo $C = P^{-1}B_1P$, važi
$AC = AP^{-1}B_1P = P^{-1}A_1PP^{-1}B_1P = P^{-1}A_1B_1P =$
$det(A)I = P^{-1}B_1A_1P = CA$ a prema jedinstvenosti adjungovane matrice mora biti $C = B = P^{-1}B_1P$, pa i $B \in R_p$. $\Diamond$

Teorema 2.3.8 *Uz oznake iz prethodnih tvrđenja, endomorfizam ϕ_A je automorfizam ako i samo ako $A\,(mod\,p) \in GL_n\mathbb{F}_p$.*

Dokaz:
$\Rightarrow$ Neka je M automorfizam, tj $M^{-1} \in EndH_p$. Postoji matrica $A \in R_p$, tako da je $M = \phi(A)$, i matrica $B \in R_p$, tako da je $M^{-1} = \phi(B)$. Uočimo $\phi(AB - I) = \phi(AB) - \phi(I) = 0$, pa $AB - I \in Ker\phi$, odnosno p deli svaki element matrice $AB - I$, iz čega obavezno $AB = I\,(mod\,p)$. Dakle:
$det(AB) = det(A)det(B) = 1\,(mod\,p)$, pa $p \nmid det(A)$, odnosno A je invertibilna, pripada $GL_n(\mathbb{F}_p)$
$\Leftarrow$ Obrnuto, neka $p \nmid det(A)$, i neka je $s \in \mathbb{Z}$ inverz za $detA$, po modulu p^{e_n}. Primetimo da osim $detAs = 0\,(mod\,p^{e_n})$, važi za sve $j \leq n$ $detAs = 0\,(mod\,p^{e_j})$. Neka je B matrica adjungovana matrici A. Tada je sB inverz od A, jer
$\phi(sBA) = \phi(AsB) = \phi(sdetAI) = I$. Lako se izvede da sB pripada R_p, čime je dokaz završen. $\Diamond$

2.4 Broj automorfizama konačne Abelove grupe

Za Abelovu grupu $H_p = \mathbb{Z}_{p^{e_1}} \times \ldots \times \mathbb{Z}_{p^{e_n}}$ broj automorfizama možemo izračunati tako što prvo pronađemo elemente iz $GL_n(\mathbb{F}_p)$ koji se mogu produžiti do matrice iz R_p koja predstavlja endomorfizam, a zatim izračunamo na koliko različitih načina to može da se uradi. Uzimajući $e_1 \leq \ldots \leq e_n$, među njima može biti istih, i bitno je da uočimo još brojeve koji broje iste elemente p^{e_i}, kao u [10], gde su elementi koji se ponavljaju predstavljeni podmatricama. Definišimo najmanji i najveći indeks u grupi istih elemenata:

$$d_k = max(l \,:\, e_l = e_k),\ c_k = min(l \,:\, e_l = e_k)$$

a zatim matricu koja predstavlja automorfizam predstavimo iz delova, prebrojimo linearno nezavisne kolone i uračunamo ih prikladno puta.

Teorema 2.4.1 *Za konačnu p-grupu $H_p = \mathbb{Z}_{p^{e_1}} \times \ldots \times \mathbb{Z}_{p^{e_n}},\ p \in Prost,\ 1 \leq e_1 \leq \ldots \leq e_n$ važi*

$$|AutH_p| = \prod_{1\leq k\leq n} (p^{d_k} - p^{k-1}) \prod_{1\leq j\leq n} (p^{e_j})^{n-d_j} \prod_{1\leq i\leq n} (p^{e_i-1})^{n-c_i+1}$$

2.5 Automorfizmi Abelovih grupa bez torzije

Grupa automorfizama grupe bez torzije ne daje puno informacija o samoj grupi. Postoje neizomorfne grupe koje imaju iste grupe automorfizama. Čak u slučaju grupa bez torzije $AutG$ može biti i konačna. U ovom odeljku biće izneta svojstva Abelovih grupa bez torzionih elemenata koja su dokazali *Hallet* i *Hirsch* [3].

Teorema 2.5.1 *Konačno generisana Abelova grupa je slobodna ako i samo ako je bez torzije.*

Dokaz: Prema teoremi o razlaganju $G \cong \mathbb{T} \times \mathbb{Z}^s$ gde je prvi član konačni proizvod konačnih grupa. Element $a = (t, b)$ je konačnog reda ako i samo ako je $b = 0$ tj. element je konačnog reda ako i samo ako je oblika $a = (t, 0)$ za $t \in \mathbb{T}$. $\Diamond$

Teorema 2.5.2 *Neka je G grupa bez torzije.*
1. Ako je $AutG$ torziona, onda $EndG$ nema nilpotentnih elemenata.
2. Ako je $AutG$ torziona, tada svaka involucija $\alpha \in AutG$ pripada njenom centru.

Dokaz:
1. Neka je $\phi \neq 0, \phi \in EndG$ za koji $\phi^2 = 0$. Tada za endomorfizme $1+\phi, 1-\phi$ važi $(1+\phi)(1-\phi) = 1$, odnosno, oni su jedan drugom inverz, pa oba pripadaju $AutG$. Ovo je torziona grupa, pa postoji n za koje $(1+\phi)^n = 1 + n\phi = 1$, ali pošto je $EndG$ bez torzije, to je moguće jedino za $\phi = 0$. Kontradikcija.
2. Neka je $\alpha \in AutG$ involucija, tj $\alpha^2 = 1$. Za proizvoljan endomorfizam β uočimo endomorfizme $\phi = (1+\alpha)\beta(1-\alpha), \psi = (1-\alpha)\beta(1+\alpha)$. Oni su nilpotentni pa prema 1. su 0, odnosno $2(\alpha\beta - \beta\alpha) = \phi - \psi = 0$, odakle $\alpha\beta = \beta\alpha$. $\Diamond$

Pre sledećeg tvrđenja biće izneta neka svojstva ciklotomičnih polinoma.

Definicija 2.5.3 *n - ti koren iz jedinice je kompleksan broj z za koji je $z^n = 1$. n - ti koren iz jedinice je primitivan ako $z^k = 1$ ne važi ni za jedno $k < n$. n - ti ciklotomični polinom $\Phi_n(x)$ je moničnI polinom $\Phi_n(x) = \prod_z (x - z)$, gde su z primitivni n - ti koreni iz jedinice. Ciklotomično polje je $\mathbb{Q}[\zeta_n]$, gde je ζ_n primitivni n - ti koren iz jedinice. To je polje razlaganja n - tog ciklotomičnog polinoma nad $\mathbb{Q}$.*

Lema 2.5.4 *$\Phi_n(x)$ je nerastavljiv u $\mathbb{Z}[x]$ i $\mathbb{Q}[x]$. Važi $\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n} \Phi_d(x)}$* $\Diamond$

Teorema 2.5.5 *Neka je G grupa bez torzije i $AutG$ torziona.*
1. Ako je $\phi \in AutG$ neparnog reda $n > 1$, tada je obavezno $n = 3$.
2. $AutG$ nema elemenata reda 8.
3. Nije svaka involucija sadržana u cikličnoj podgrupi reda 12

Dokaz:
1. Dovoljno je pokazati za $n = p^k$, gde je $p \in Prost, p \geq 3$. Uočimo endomorfizam $\beta = 1 - \phi + \phi^2 - \ldots + \phi^{n-3}$. Za $n \equiv 1(mod4)$ β ima inverz $\phi^2 - \phi^4 + \ldots \phi^{n+1}$, a za $n \equiv 3(mod4)$ β ima inverz $\phi^3 - \phi^5 + \ldots \phi^n$, dakle pripada $AutG$, pa je konačnog reda. Primetimo da je za $x \in G, \phi^n - 1(x) = 0$, pa postoji i minimalni polinom $\mu(x)$ sa celim koeficijentima koji poništava svaki element iz G. n - ti ciklotomični polinom Φ_n je nerastavljiv u $\mathbb{Z}[x]$ i deli polinom $\mu(x)$. Uočimo preslikavanje $\phi \to \zeta$, (gde je ζ n - ti primitivni koren iz jedinice) iz prstena generisanog sa ϕ u ciklotomično polje $\mathbb{Q}[\zeta]$. Ovo je homomorfizam prstena. β je generisano sa ϕ i njegova slika pri ovom preslikavanju je $1 - \zeta + \zeta^2 - \ldots + \zeta^{n-3} = (1 + \zeta^{n-2})(1 + \zeta)^{-1}$, čiji je moduo jednak 1 u slučaju da $\zeta^{n-2} = \zeta$ ili $\zeta^{n-2} = \overline{\zeta}$, a to je za $n = 3$. U svim ostalim slučajevima je red β beskonačan pa β ne pripada torzionoj grupi $AutG$.
2. Pretpostavimo da postoji element α reda 8 i uočimo $\beta = 1 + (1 - \alpha^4)(1 + \alpha - \alpha^3)$ i $\gamma = 1 + (1 - \alpha^4)(1 - \alpha + \alpha^3)$, oni su jedan drugom inverz. Kao malopre uočimo homomorfizam iz prstena generisanog sa α u $\mathbb{Q}[\zeta]$, gde $\zeta = \frac{1+i}{\sqrt{2}}$, primitivni osmi koren iz jedinice. Tada je slika elementa β $3 + 2\sqrt{2}$, što je element beskonačnog reda u $\mathbb{Q}[\zeta]$.
3. se dokazuje analognim postupkom. $\Diamond$

Definicija 2.5.6 *Podgrupa H grupe G naziva se karakteristična ili (invarijantna) ako je fiksira svaki automorfizam grupe G, i potpuno karakteristična (potpuno invarijantna) ako je fiksira svaki endomorfizam grupe G.*

Sledeće tvrđenje ćemo iskoristiti bez dokaza:

Lema 2.5.7 *Neka je G grupa bez torzije i $\alpha, \beta \in EndG$. Pretpostavimo:*
1. $\alpha\beta = 0$
2. levi ideal prstena $EndG$ generisan sa α i β sadrži $mEndG$ za neki ceo broj $m > 0$
3. $EndG$ nema nilpotentnih elemenata različitih od 0.
Tada su $Ker\alpha$ i $Ker\beta$ potpuno karakteristične podgrupe od G i važi $mG \leq Ker\alpha \oplus Ker\beta$ $\Diamond$

Teorema 2.5.8 *Neka je G grupa bez torzije.*
1. Ako je $AutG$ torziona, tada su njene Silovljeve 3 - podgrupe komutativne
2. Ako je $\alpha \in AutG$ involucija, onda G ima karakterističnu podgrupu H za koju važi: ako je $\phi : AutG \to AutH$ restrikcija automorfizma grupe G na H, tada je $\phi(\alpha) = -1$ i $|\phi(AutG)|$ deli 24

Dokaz:
1. Neka je $S \leq AutG$ Silovljeva 3 - podgrupa, i $\alpha, \beta \in S$, i komutator $\gamma = \alpha^{-1}\beta^{-1}\alpha\beta$. Prema nekom od prethodnih tvrđenja ovi elementi su reda 3, tj $\alpha^3 = \beta^3 = \gamma^3 = 1$, i $\alpha\gamma = \gamma\alpha$, $\beta\gamma = \gamma\beta$. Primenimo lemu 2.5.7 sa vrednostima $1 + \gamma + \gamma^2$, $1 - \gamma$, $m = 3$, dobijamo $3G \leq B \oplus C$, gde su $B = Ker(1+\gamma+\gamma^2)$, $C = Ker(1-\gamma)$ potpuno invarijantne u G. Slično i $3B \leq [Ker(1+\alpha+\alpha^2) \cap B] \oplus [Ker(1-\alpha) \cap B]$. Ovde α indukuje identitet na drugom sabirku, i on je sadržan u C. Dakle

$$
\begin{aligned}
&(1 + \alpha + \alpha^2)(1 - \gamma) = 0 \Rightarrow \\
&\gamma + \gamma\alpha + \gamma\alpha^2 = 1 + \alpha + \alpha^2 \Rightarrow \\
&\gamma + \gamma^2\alpha + \alpha^2 = 1 + \gamma\alpha + \gamma^2\alpha^2 \\
&(\beta^{-1}\alpha\beta = \gamma\alpha, \gamma^3 = 1) \\
&\gamma + \alpha + \gamma^2\alpha^2 = 1 + \gamma^2\alpha + \gamma\alpha^2 \Rightarrow \\
&3\gamma = 3 \Rightarrow \gamma = 1
\end{aligned}
$$

Dakle, S je komutativna.
2. Primenimo lemu 2.5.7 sa vrednostima $1 - \alpha, 1 + \alpha, m = 2$, dobijamo $2G \leq B_1 \oplus C_1$, gde je B_1 potpuno invarijantna. Neka je $\phi_1 : AutG \to AutB_1$. Element $\phi_1(\alpha)$ je reda 2. Ako bi postojao još neki element reda 2 u $\phi_1(AutG)$, primenili bismo postupak ponovo i dobili $2B_1 \leq B_2 \oplus C_2$, i na kraju dobili karakterističnu podgrupu B_0 za koju je $\phi_0(\alpha)$ jedini element reda 2 u $\phi_0(AutG)$. To znači da su Silovljeve 2 - podgrupe grupe $\phi_0(AutG)$ ciklične reda 2 ili 4 ili grupe kvaterniona. Zato red $|\phi_0(AutG)| = 2^k 3^l, k \leq 3$. Ako je $l > 1$, odaberimo element δ reda 3 i primenimo lemu 2 sa vrednostima $1+\delta+\delta^2, 1-\delta, m = 3$, dobijamo $3B_0 = B^{'} \oplus C^{'}$ za koje $1+\delta+\delta^2|_{B'} = 0, \delta|_{C'} = 1$, ako postoji još neki element reda 3 nastavimo dok ne dobijemo karakterističnu podgrupu B za koju $1 + \beta + \beta^2 = 1 + \gamma + \gamma^2 = 0$ za svaka dva elementa β, γ iz Silovljeve 3 - podgrupe od $\phi(AutG)$. Ako je $\gamma \neq \beta^{-1}$, onda $1 + \beta\gamma + (\beta\gamma)^2 = 0$ u B. Tada $-\beta\gamma = 1 + \beta^2\gamma^2 = 1 + (1 + \beta)(1 + \gamma) = 2 + \beta + \gamma + \beta\gamma$. Pošto $(\beta - \gamma)^2 = 0$ i $EndG$ nema nilpotentnih elemenata, sledi $\beta = \gamma$, odnosno Silovljeve 3 - podgrupe od $\phi(AutG)$ su reda 3, pa $|\phi(AutG)|$ deli 24. $\Diamond$

Teorema 2.5.9 *U grupama $\mathbb{Z}_{12}, DC_{24} =< a, b|a^6 = b^2 = (ab)^2 >$ ne važi tvrđenje 2.5.5, pod 3.*

Dokaz: Neka je $\alpha \in AutG$ reda 12. Tada $\alpha^{12} - 1$ poništava svaki element iz G i postoji minimalni polinom sa celim koeficijentima $\mu(x)$, koji deli $x^{12} - 1$. Međutim, ciklotomični polinom Φ_{12} ne deli $\mu(x)$, jer pri preslikavanju koje slika α u dvanaesti primitivni koren iz jedinice, element $1 + \alpha$ se slika u kompleksan broj čiji je moduo različit od 1. $\Diamond$

Teorema 2.5.10 *(Hallet i Hirsch) Ako je konačna grupa A grupa automorfizama grupe bez torzije G, tada je ona izomorfna podgrupi konačnog proizvoda sledećih grupa:*
1. ciklična grupa reda $2, 4$ ili 6
2. grupa kvaterniona $Q_8 =< a, b|a^2 = b^2 = (ab)^2 >$
3. diciklična grupa reda 12 $DC_{12} =< a, b|a^3 = b^2 = (ab)^2 >$
4. binarna tetraedarska grupa reda 24 $BT_{24} =< a, b|a^3 = b^3 = (ab)^2 >$

Dokaz: Primenićemo postupak od malopre i zaključiti da za neko $m, mG \leq C_1 \oplus \ldots \oplus C_k$ gde su C_i karakteristične podgrupe od G za koje $\phi_i : AutG \to C_i$ $|\phi_i(AutG)|$ deli 24. Uočimo homomorfizam $\psi : AutG \to \phi_1(AutG) \times \ldots \times \phi_k(AutG)$, koji slika $\alpha \to (\phi_1\alpha, \ldots, \phi_k\alpha)$. Sve grupe čiji red deli 24, i zadovoljavaju uslove tvrđenja 2.5.2, pod 2, tvrđenja 2.5.5, pod 2, i tvrđenja 2.5.9, su upravo grupe navedene u teoremi, čime je dokaz završen. $\Diamond$

Teorema 2.5.11 *(Hallet i Hirsch) Neka je G slobodna Abelova grupa. Ako je $AutG \cong DC_{12}$, onda je $rang(G)$ paran, a ako je $AutG \cong Q_8$, i $AutG \cong BT_{24}$, onda je $rang(G)$ deljiv sa 4.*

Dokaz: Najpre kažimo neka svojstva grupe DC_{12}. Jedini element reda 2 je $\alpha^2 = \beta^3 = (\alpha\beta)^2$ i on predstavlja automorfizam koji elementu x dodeli $-x$. Za svako $g \in G, g \neq 0$ možemo uočiti da su g i $\alpha(g)$ linearno nezavisni: $ag + b\alpha(g) = 0$ primenimo α: $a\alpha(g) - bg = 0$. Napišimo ovo u matričnom obliku: $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} g \\ \alpha(g) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ Dakle determinanta sistema mora biti 0, odnosno $a^2+b^2 = 0 \;\Rightarrow\; a = b = 0$. Neka je $G_1 =< g_1, \alpha(g_1) >$. Ako G/G_1 ima torzionih elemenata onda je G ranga 2. U suprotnom odaberimo element g_2 koji nije generisan sa g_1 i $\alpha(g_1)$, i stavimo $G_2 =< G_1, g_2, \alpha(g_2) >$. Ovaj proces se nastavlja dokle god količnička grupa nema torzionih elemenata i pritom se rang svaki put povećava za 2. Što se tiče Q_8, ponovo je $\alpha^2 = \beta^2 = (\alpha\beta)^2$ jedini element reda 2 i mora da predstavlja množenje sa -1. Analogno zaključujemo da su $g, \alpha(g), \beta(g), (\alpha\beta)(g)$ linearno nezavisni i rang od G je umnožak od 4. U grupi BT_{24} je opet $\alpha^3 = \beta^3 = (\alpha\beta)^2 = -1$, i sa odgovarajućim uslovima se dobije da su $\alpha(g), \beta(g), (\alpha\beta)(g)$ linearno nezavisne i rang od G je umnožak od 4. $\Diamond$

Pomenute grupe Q_8, DC_{12}, BT_{24} imaju i reprezentaciju pomoću kvaterniona preciznije, mogu se uočiti kao podgrupe multiplikativne grupe algebre kvaterniona H. To je četvorodimenziona normirana algebra nad $\mathbb{R}$, tačnije, skup $\mathbb{R}^4$ sa standardnim sabiranjem i množenjem skalarima, sa odgovarajuće definisanim množenjem i normom. Za množenje je neophodno odabrati bazu od $\mathbb{R}^4$, $1, i, j, k$, definisati množenje baznih elemenata, i preko njih i množenje ostalih elemenata. Irski matematičar Ser Vilijam Roen Hamilton (*William Rowan Hamilton*) tragajući za pogodnim prikazom tačaka u prostoru, uveo je kvaternione godine 1843. Poznata je priča o trenutku u kome mu je sinula ideja o množenju baznih elemenata tokom šetnje pored mosta Brum, gde je urezao relacije

$$i^2 = j^2 = k^2 = ijk = -1$$

Dakle, tačke u prostoru se mogu prikazati i na ovaj način, a sva kretanja kao automorfizmi koji čuvaju celokupnu strukturu. Norma dozvoljava očuvanje dužina i uglova. Ono što je posebno zanimljivo je pitanje kako isprogramirati kretanje bilo koje vrste. Možemo primetiti da je $\mathbb{R}^4$ Abelova grupa ali ona nije konačno generisana. Međutim, u softverskim simulacijama zapravo na raspolaganju imamo samo konačno mnogo realnih brojeva. Detaljnije o značaju kvaterniona u kompjuterskoj grafici, bioinformatici, molekularnoj fizici i svakoj oblasti koja kompjuterski simulira kretanja u prostoru biće opisano u trećoj glavi.

2.6 Opšti slučaj

Što se tiče automorfizama mešovitih konačno generisanih Abelovih grupa, jedan način da se oni odrede je posmatranjem da li data grupa zadovoljava neka opšta svojstva, a da su u tim slučajevima poznata svojstva automorfizama ili struktura grupe automorfizama.

U pokušaju pronalaženja odgovora na pitanja o strukturi grupe automorfizama, i njenom uticaju na samu grupu, primenjuju se razne metode. Važi $AutG = EndG^*$, pa vidimo da o samoj grupi G možemo više zaključiti posmatrajući $EndG$, dok posmatranje grupe $AutG$ dozvoljava primenu drugačijih metoda u nadi da se dobiju bolji rezultati. U ovom odeljku biće razmotren samo jedan mali deo mogućnosti: na koje načine proučavanje konačno generisanih Abelovih grupa doprinosi proučavanju opštih slučajeva. Prirodno je posmatrati endomorfizme preko matrica, kao što smo videli u slučaju konačno generisanih Abelovih grupa, i voleli bismo da primenimo slična razmatranja u opštijim slučajevima. U slučaju beskonačno generisanih grupa to je moguće uvođenjem konačne topologije na skupu $EndG$.

Definicija 2.6.1 *Topologija na skupu X je kolekcija Ω podskupova tog skupa koja obavezno sadrži uniju proizvoljno mnogo elemenata, presek konačno mnogo elemenata iz Ω, kao i ceo X i prazan skup. Elementi kolekcije Ω nazivaju se otvoreni skupovi.*

Za proizvoljnu grupu G uvedimo na skupu $EndG$ kolekciju otvorenih skupova koja zavisi od G. Topologija se može definisati preko sistema okolina, okolina neke tačke je skup koji sadrži otvoren skup kome pripada ta tačka.

Definicija 2.6.2 *Za konačan podskup $X \subset G$, X - okolina elementa $\alpha \in EndG$ definiše se kao skup*

$$U_X(\alpha) = \{\beta \in EndG : \beta(x) = \alpha(x), za\, sve\, x \in X\}$$

Topologija određena na ovaj način naziva se konačna topologija.

Svi ostali pojmovi (konvergencija, kompaktnost, povezanost...) mogu se definisati preko otvorenih skupova.

Definicija 2.6.3 *Matrica $[\alpha_{ij}]$ sa elementima iz EndG naziva se "konvergentna po kolonama" ako za svaku kolonu j suma $\sum_i \alpha_{ij}$ postoji u konačnoj topologiji na skupu EndG.*

Neka je $G = \bigoplus_{i\in I} G_i$ i ϵ_i odgovarajuće projekcije posmatrane kao endomorfizmi koji slikaju $\epsilon_i : a = (a_1, \ldots, a_i, \ldots) \to (0, \ldots, 0, a_i, 0, \ldots)$. Svako $a \in G$ se može napisati $a = \sum_i \epsilon_i(a)$, i za svako $\alpha \in EndG$, $\alpha(a) = \sum_i (\alpha\epsilon_i)(a) = \sum_{i,j} (\epsilon_i \alpha \epsilon_j)(a)$. Na ovaj način, svakom endomorfizmu odgovara matrica $[\alpha_{ij}]$ gde $\alpha_{ij} = \epsilon_i \alpha \epsilon_j$. Lako se proveri da je preslikavanje koje slika ovaj endomorfizam u odgovarajuću matricu homomorfizam prstena.

Teorema 2.6.4 *Neka je $G = \bigoplus_{i\in I} G_i$. Tada je EndG izomorfan prstenu matrica "konvergentnih po kolonama" $[\alpha_{ij}]$, gde $\alpha_{ij} \in Hom(G_j, G_i)$.*

Dokaz: Za svaku kolonu j, $\sum_i \alpha_{ij} a = (\alpha\epsilon_j)(a)$, odnosno, matrica je konvergentna po kolonama, i obrnuto. Dalje, uočimo podgrupu $\epsilon_i EndG \epsilon_j$, ona odgovara $Hom(G_j, G_i)$. $\Diamond$

Teorema 2.6.5 *Neka je $G = \bigoplus_{i\in I} G_i$. Tada grupa automorfizama odgovara invertibilnim matricama konvergentnih po kolonama.* $\Diamond$

Primetimo ako je G konačno generisana Abelova grupa, svaki podskup od G je otvoren, odnosno, ova topologija je *diskretna*.

3 Primeri i primene

3.1 Dejstvo grupe Aut(G) na G

Definicija 3.1.1 *Neka je X skup i G grupa. Dejstvo grupe G na skup X je preslikavanje* $(g, x) \to gx, G \times X \to X$ *za koje je ispunjeno*

$$\forall x \in X,\ 1x = x$$
$$\forall g_1, g_2 \in G, x \in X,\ (g_1 g_2)x = g_1(g_2 x)$$

Za neko $g \in G$ uočimo levu translaciju $g_L : x \to gx$, ovo preslikavanje ima inverz $(g^{-1})_L$, to je bijekcija, odnosno $g_L \in Sym(X)$. Iz drugog svojstva sledi da je $g \to g_L : G \to Sym(X)$ homomorfizam, tačnije svako levo dejstvo određuje ovakav homomorfizam, i obrnuto, homomorfizam indukuje levo dejstvo G na X. U slučaju da je X grupa, među bijekcijama iz $Sym(X)$ ima i automorfizama, pa sledeće tvrđenje lako sledi.

Lema 3.1.2 *Za svaku grupu G, AutG dejstvuje na G.* $\Diamond$

Ovakav način posmatranja je pogodan za primene u kombinatornim problemima prebrojavanja, u kriptografiji, kristalografiji, i mnogim drugim oblastima. Posebno, pri rešavanju problema u kojima je bitno prebrojati orbite i elemente stabilizatora mnogo rezultata daje teorija Polija, i primena Burnsajdove leme. Naravno, ti rezultati važe za proizvoljne skupove, a mogu se primeniti na grupe. Samo jedna od primena može se uočiti u faktorizaciji grupe $\mathbb{Z}_n$ koristeći dejstvo $Aut\mathbb{Z}_n = \Phi_n$ [8]. U tom radu je izneta sledeća ideja: dejstvo $(g, x) \to gx, x \in \mathbb{Z}_n, g \in \Phi_n$ se prirodno može produžiti do dejstva na skupu podskupova od $\mathbb{Z}_n$ veličine k. Svaka permutacija na nekom skupu može se predstaviti preko ciklusa, za grupu permutacija to predstavljanje opisuje ciklični indeks. Nađe se stabilizator skupa veličine k, a odatle lako i orbita kojoj pripada taj skup. Zatim se ti rezultati koriste u pronalaženju faktorizacija grupe G čiji su faktori podskupovi, ne obavezno podgrupe.

Tehnike u tom radu opisuju i kako se problem pločanja ravni, poznata hipoteza Minkovskog može preformulisati u terminima konačnih Abelovih grupa. Hajos je 1942 dao konačan odgovor na to pitanje, što je imalo ogroman uticaj na tu oblast, i pospešilo istraživanja u tom smeru.

3.2 Grupe bez torzije G sa određenim Aut(G)

Dokazali smo šta sve mogu biti grupe automorfizama Abelovih grupa bez torzije. Ovde će biti pokazani primeri grupa sa konačnom prezentacijom (konačno mnogo generatora i relacija) čije su grupe automorfizama $\mathbb{Z}_2, \mathbb{Z}_4, DC_{12}, BT_{24}$. Pritom, možemo uočiti pogodan način da proizvoljnu grupu bez torzije (ne obavezno konačno generisanu) predstavimo kao proširenje slobodne neke slobodne grupe $F =< f_1, \ldots, f_r >$ ranga r. Dodaćemo još proizvoljno generatora za koje zahtevamo da važe relacije definisane na sledeći način:

$$G =< F, g_i, i = 1, 2, \ldots | p_i g_i = l_i(f_1, \ldots, f_r) >$$

gde su $p_i \in Prost$, a $p_i g_i$ linearne kombinacije generatora f_j. Ovako definisane relacije pokazuju da neki elementi iz F treba da budu deljivi sa p_i, što znači da važe neke kongruencije za koeficijente iz l_i i to uslovljava izgled automorfizama. Ovo će biti jasnije kroz primere. Neka je $\gamma \in AutG$. Tada

$$\gamma(p_i g_i) = \gamma(l_i(f_1, \ldots, f_r)) = l_i(\gamma(f_1), \ldots, \gamma(f_r)) = p_i \gamma(g_i)$$

pa ako je ovaj element iz F deljiv sa p_i, onda je $\gamma(g_i) = h_i$. Slika od f_j je

$$\gamma(f_j) = \sum_{1 \le i \le r} x_{ij} f_i + \sum_{i=1,2,\ldots} y_{ij} g_i = \sum_{1 \le i \le r} x_{ij} f_i + \sum_{i=1,2,\ldots} y_{ij} \frac{1}{p_i} l_i(f_1, \ldots f_r)$$
$$\gamma(f_j) = \sum_{1 \le i \le r} a_{ij} f_i$$

gde je prva suma konačna a druga beskonačna i skoro svi y_{ij} jednaki nuli, pa automorfizmu γ mozemo pridružiti matricu (a_{ij}) sa racionalnim elementima koji u imeniocu imaju samo po jedan od brojeva p_i. Ako zahtevamo još da F bude karakteristična podgrupa od G, tada su svi $y_{ij} = 0$, i matrica je sa celobrojnim elementima. Time dobijamo automorfizme od F koji su produženi na dodatne generatore g_i. Ovakav pristup su izveli *J. T. Hallet* i *K. A. Hirsch* [3]

$\mathbb{Z}_2$ **kao grupa automorfizama:** Neka je F slobodna grupa ranga 1, tada jasno $Aut(F) = \mathbb{Z}_2$. Uočimo $G =< f, g_i, i = 1, 2, \ldots | p_i g_i = f >$ i to su te grupe.

$\mathbb{Z}_4$ **kao grupa automorfizama:** Neka su $p_i = 1\,(mod\,4), p_i = x_i^2 + y_i^2, x_i > y_i > 0$, i slobodna Abelova grupa ranga 2 $F =< f_1, f_2 >$. Definišimo $G =< F, d_i, i = 1, 2, \ldots | p_i d_i = x_i f_1 + y_i f_2 >$. Biće $AutG \cong \mathbb{Z}_4$. Najpre ćemo pokazati da je G bez torzije:

Neka je $g \in G$, i $\phi : G \to G/F$. Dovoljno je da dokažemo da iz $p_i g = 0$ sledi $g = 0$. Ako je p_i red od $\phi(g)$ u G/F, to znači da je $p_i g \in F$. Ovi koseti su određeni slikama d_i, pa slika od g pripada nekom od njih, odnosno, g je oblika $g = a_1 f_1 + a_2 f_2 + b d_i$, jer $p_i d_i \in F$. Dakle,

$$p_i g = p_i(a_1 f_1 + a_2 f_2 + b d_i) = p_i a_1 f_1 + p_i a_2 f_2 + b p_i d_i = \\ = p_i a_1 f_1 + p_i a_2 f_2 + b(x_i f_1 + y_i f_2) = f_1(p_i a_1 + b x_i) + f_2(p_i a_2 + b y_i)$$

Iz linearne nezavisnosti, ako je $p_i g = 0$ sledi da su ovi koeficijenti jednaki nuli, a to je moguće jedino za $a_1 = a_2 = b = 0$, pa time i $g = 0$.

Dalje, odredićemo elemente iz F koji su deljivi sa datim p_i, da bismo odredili automorfizme od G. Neka je $f = a_1 f_1 + a_2 f_2 = p_i g$ deljivo sa p_i. Ako je slika elementa g pri ϕ neutral u G/F, to znači da je $g \in F$, i upoređivanjem koeficijenata lako sledi $p_i | a_1, a_2$. Ako $\phi(g) \neq 0$, to znači da je $g = f + \sum_i b_i d_i$, i skoro svi $b_i = 0$. Ako $p_i g \in F$, onda za sve $j \neq i$ su koeficijenti b_j deljivi sa p_j, i čine neki element iz F, tačnije $g = f^* + b_i d_i$, a b_i nije deljivo sa p_i jer $g \notin F$. Dalje,

$$p_i g = a_1 f_1 + a_2 f_2 = p_i f^* + b_i p_i d_i = p_i f^* + b_i(x_i f_1 + y_i f_2)$$

Odavde $a_1 = b_i x_i\,(mod\,p_i), a_2 = b_i y_i\,(mod\,p_i)$, ili drugačije $y_i a_1 = x_i a_2\,(mod\,p_i)$. I obrnuto, kada je ispunjeno prethodno za a_1, a_2, $f = a_1 f_1 + a_2 f_2$, važi

$$x_i f = x_i a_1 f_1 + x_i a_2 f_2 = x_i a_1 f_1 + (y_i a_1 + k p_i) f_2 = a_1(x_i f_1 + y_i f_2) + k p_i f_2$$

$x_i f$ je deljivo sa p_i, ali $(x_i, p_i) = 1$, pa je obavezno f deljivo sa p_i. Time smo pokazali potreban i dovoljan uslov da element iz F bude deljiv sa p_i. Neka je najzad, $\gamma \in Aut(G)$. Tada je

$$\gamma(f_1) = a_{11} f_1 + a_{12} f_2$$
$$\gamma(f_2) = a_{21} f_1 + a_{22} f_2$$

sa racionalnim koeficijentima čije relacije ćemo sada odrediti. Uzmimo najmanji zajednički sadržalac od njihovih imenioca, m, tako da $b_{ij} = m a_{ij}$ budu celi brojevi. Za svako $f \in F, \gamma(mf) \in F$ posebno za svako p_i i odgovarajuće x_i, y_i $\gamma(m(x_i f_1 + y_i f_2))$ pripada F i deljivo je sa p.

$$\gamma(m(x_i f_1 + y_i f_2)) = (x_i b_{11} + y_i b_{21}) f_1 + (x_i b_{12} + y_i b_{22}) f_2$$

Primenimo kriterijum od malopre $y_i(x_i b_{11} + y_i b_{21}) = x_i(x_i b_{12} + y_i b_{22})\,(mod\,p_i)$ dobijamo

$$y_i(b_{11} - b_{22}) = x_i(b_{12} + b_{21})\ (mod\,p_i)$$
$$(b_{11} - b_{22})^2 + (b_{12} + b_{21}) = 0\ (mod\,p_i)$$

ali izraz sa leve strane je fiksirani broj dok p_i može biti proizvoljno veliko. Zato je $b_{11} = b_{22}, b_{12} = -b_{21}$, i matrica našeg automorfizma je $\frac{1}{m}\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ Sada želimo da pokažemo da je F karakteristična podgrupa od G, što znači da je $m = 1$. Jedini prosti delioci od m su p_i. Pretpostavimo da je $m > 1, p = x^2 + y^2 | m$.

$$\gamma(mf_1) = af_1 + bf_2 = 0\,(mod\,p),\ ya = xb\,(mod\,p)$$
$$\gamma(m(xf_1 + yf_2)) = p^2 g,\ pg \in F$$
$$\gamma(m(xf_1 + yf_2)) = x(af_1 + bf_2) + y(-bf_1 + af_2) = (xa - yb)f_1 + (xb + ya)f_2$$
$$xa - yb = xb + ya = 0\,(mod\,p)\ \Rightarrow\ a = b = 0\,(mod\,p)$$

Zato mora biti $m = 1$. Jednačina $a^2 + b^2 = 1$ ima četiri rešenja, koja čine cikličnu grupu reda 4. Ako odaberemo $a = 1, b = 0$, to je identitet, a generator je $a = 0, b = 1$.

Primedba: Analogno se može izvesti slučaj $\mathbb{Z}_6$, s tim da biramo

$$p_i = 1\,(mod\,6), p_i = x_i^2 + x_i y_i + y_i^2$$

Q_8 kao grupa automorfizama: Već smo pokazali da u slučaju $Aut(G) \cong Q_8$ rang grupe G deljiv sa 4. Neka je slobodna grupa ranga 4 $F =< f_1, f_2, f_3, f_4 >$, i prosti brojevi $p_i, q_j = 1\,(mod\,4)$, $p_i = x_i^2 + y_i^2, q_j = z_j^2 + w_j^2$ i neka je $G =< F, d_{i1}, d_{i2}, d_{j1}, d_{j2}, i, j = 1, 2, \ldots >$ i relacije

$$p_i d_{i1} = x_i f_1 + y_i f_2 \;\; p_i d_{i2} = x_i f_4 + y_i f_3$$
$$q_j d_{j1} = z_j f_1 + w_j f_3 \;\; q_j d_{j2} = z_j f_2 + w_j f_3$$

Kriterijum za deljivost sa p_i je $y_i a_1 = x_i a_2, y_i a_4 = x_i a_3\,(mod\,p_i)$ a sa q_j q_j je $w_j a_1 = z_j a_3, w_j a_2 = z_j a_4\,(mod\,q_j)$. Sada automorfizmu γ odgovara matrica $\frac{1}{m}(a_{ij})$ za čije koeficijente se dobija

$$a_{22} = a_{11},\; a_{21} = -a_{12}, a_{24} = -a_{13},\; a_{23} = a_{14}$$
$$a_{42} = -a_{31},\; a_{41} = a_{32}, a_{44} = -a_{33},\; a_{43} = -a_{34}$$

3.3 Prostorne rotacije i kvaternioni

Neka su $1 = (1,0,0,0), i = (0,1,0,0), j = (0,0,1,0), k = (0,0,0,1)$. Posmatrajmo strukturu $(\mathbb{R}^4, +, \cdot_\lambda, \cdot_q)$, gde osim množenja skalarima iz $\mathbb{R}$ postoji i množenje $\cdot_q$ opisano na elementima $1, i, j, k$:

$$i^2 = j^2 = k^2 = ijk = -1$$

Uvedemo li normu, $\|q\| = \sqrt{a^2 + b^2 + c^2 + d^2}$, dobijamo normiranu deljivu algebru kvaterniona. Prema teoremi Frobeniusa, to je jedna od dve konačno generisane algebre nad $\mathbb{R}$ (druga je $\mathbb{C}$).

Samo jedna od mogućih primena kvaterniona je u opisivanju i programiranju kretanja. Svako kretanje se može razložiti na rotaciju i translaciju. U ovom odeljku biće opisana primena kvaterniona u prikazivanju rotacija, razlozi korišćenja i potencijalna poboljšanja postojećih algoritama.

Prikazaćemo prostor rotacija najpre na jednostavnijem primeru rotacije u trodimenzionom prostoru oko ose koja leži u xy ravni za ugao α. Takvoj rotaciji pridružimo krug sa poluprečnikom koji odgovara veličini ugla α. Možemo uočiti taj krug na sferi, što je ugao rotacije manji, to je krug bliži severnom polu. Kako se ugao povećava i približava π, tako se i poluprečnik kruga povećava do ekvatora, a zatim smanjuje do južnog pola. Dakle, severnom i južnom polu odgovara jedinično preslikavanje, a svaka rotacija je predstavljena pomoću dve antipodalne tačke na sferi. Takav prikaz omogućava da se rotacija predstavi pomoću ose u dva smera. Uopštimo ovo na sledeći način: jedinična rotacija je tačka, rotacija za mali ugao je sfera malog poluprečnika, na hipersferi u četvorodimenzionom prostoru. Ovo se odlično prikazuje jediničnim kvaternionima. Neka je $q = a + bi + cj + dk$, tako da $q^2 = -1$. To znači $a^2 - b^2 - c^2 - d^2 = -1, 2ab = 0, 2ac = 0, 2ad = 0$, odnosno, $a = 0, b^2 + c^2 + d^2 = 1$. Dakle, kvaternioni sa realnim delom jednakim nuli a imaginarnim delom koji kao vektor iz $\mathbb{R}^3$ ima normu 1, čine jediničnu sferu.

Sfera u trodimenzionom prostoru se može parametrizovati na razne načine pomoću dva parametra, ali svaki od njih ima tačke u kojima se ispoljava prekidnost. U tri koordinate, tačka na sferi (w, x, y) predstavlja rotaciju oko ose u xy ravni koja je zadata vektorom $(x, y, 0)$ za ugao $\alpha = 2arccosw = 2arcsin\sqrt{x^2 + y^2}$. Na isti način, hipersfera se može parametrizovati sa tri ugla - Ojlerovi uglovi, ali to dovodi do prekidnosti, što se može izbeći u četiri koordinate: (w, x, y, z) predstavlja rotaciju oko ose (x, y, z) za ugao $\alpha = 2arccosw = 2arcsin\sqrt{x^2 + y^2 + z^2}$

Sada će biti pokazano kako multiplikativna grupa kvaterniona dejstvuje na $\mathbb{R}^3$.

Teorema 3.3.1 *Neka je sa (w, x, y, z) predstavljena rotacija na prethodno opisan način. Uočimo kvaternion $q = w + xi + yj + zk = cos(\frac{\alpha}{2}) + \overrightarrow{u}\,sin(\frac{\alpha}{2})$, $\overrightarrow{u}$ jedinični. Za proizvoljan vektor $\overrightarrow{v}$, proizvod $\overrightarrow{v'} = q\overrightarrow{v}q^{-1}$ predstavlja vektor nakon rotacije za ugao α oko ose $\overrightarrow{u}$.*

Dokaz: Dovoljno je pokazati da je prema Rodrigezovoj formuli rotacije

$$q\overrightarrow{v}q^{-1} = \overrightarrow{v}cos\alpha + (\overrightarrow{u} \times \overrightarrow{v})sin\alpha + \overrightarrow{u}(\overrightarrow{u} \circ \overrightarrow{v})(1 - cos\alpha)$$

što jednostavnom zamenom i primenom pravila lako sledi. $\Diamond$

Teorema 3.3.2 *Proizvod kvaterniona je kompozicija rotacija. Inverz kvaterniona je inverzna rotacija. Uopšte, q^n predstavlja rotaciju za ugao n puta veći.*

Dokaz:

$$(pq)\overrightarrow{v}(pq)^{-1} = p(q\overrightarrow{v}q^{-1})p^{-1}$$
$$p^{-1}(p\overrightarrow{v}p^{-1})p = p(p^{-1}\overrightarrow{v}p)p^{-1} = \overrightarrow{v} \qquad \Diamond$$

Prednosti prikazivanja rotacija pomoću kvaterniona su brojne. Prvo, za kvaternion je potrebno četiri broja, a za matricu devet. Zatim, iz koeficijenata kvaterniona lako se dobijaju ugao i osa, i obrnuto, dok je kod matrica ili Ojlerovih uglova to komplikovanije. Takođje, prilikom kompozicije rotacija greške zaokruživanja se akumuliraju, i ako matrica koja predstavlja rotaciju odstupi od ortogonalne, teško se ponovo može namestiti, dok kvaternion koji malo odstupa od traženog dovoljno je da se normira i greška je manja.

Dalje, u kompjuterskoj animaciji neophodno je da se rotacija odvija što je ujednačenije moguće, sa što neprimetnijim diskretnim korakom - "seckanjem". Način za prevazilaženje tog problema je sferna linearna interpolacija. To je dosta jednostavnije postići pomoću kvaterniona. Još jedan problem koji se javlja korišćenjem Ojlerovih uglova ("gimbal lock") se uspešno prevazilazi kvaternionima. [11]

Literatura

[1] Christopher J. Hillar i Darren L. Rhea, *Automorphisms of Finitely Generated Abelian Groups*, Amer. Math. Monthly, 2007

[2] Laszlo Fuchs, *Abelian Groups Vol II*, 1973

[3] J.T. Hallett and K. A. Hirsch, *Die Konstruktion von Gruppen mit vorgeschriebenen Automorphismengruppen*, 1970

[4] Žarko Mijajlović, *Algebra 1, predavanja*

[5] Gojko Kalajdžić, *Linearna algebra*, Matematički fakultet, 2001

[6] Gojko Kalajdžić, *Algebra*, Matematički fakultet, 2008

[7] J. S. Milne, *Group Theory*, 2003

[8] Vladimir Božović, *Algebraic and Combinatorial Aspects of Group Factorisations*, doktorska teza, Florida Atlantic University Boca Raton, 2008

[9] K. A. Hirsch and H. Zassenhaus, *Finite Automorphism Groups of Torsion - Free Groups*, J. London Math. Soc , 1966

[10] Kenjiro Shoda, *Automorphismen Abelscher Gruppen*, 1928

[11] Ken Shoemake, *Quaternions*, Department of Computer and Information Science, University of Pennsylvania, 1994

[12] http://www.j3d.org