Konačne jednostavne grupe

Andrašec, Lucija

Sveučilište u Rijeci

Fakultet za matematiku

Sveučilišni prijediplomski studij Matematika

Lucija Andrašec

Konačne jednostavne grupe

Završni rad

Rijeka, srpanj, 2023.

Sveučilište u Rijeci

Fakultet za matematiku

Sveučilišni prijediplomski studij Matematika

Lucija Andrašec

Konačne jednostavne grupe

Završni rad

Mentor: izv. prof. dr. sc. Andrea Švob

Rijeka, srpanj, 2023.

Sadržaj

Sažetak

Grupe su zanimljive matematičke strukture koje imaju široku primjenu u matematici i fizici. U ovom radu navest ćemo neke bitne definicije i teoreme vezane uz konačne grupe. Spomenut ćemo Sylowljeve podgrupe i Sylowljeve teoreme te ćemo se susresti sa konačnim jednostavnim grupama. Njih ćemo klasificirati na cikličke grupe prostog reda, alternirajuće grupe A_n, $n \geq 5$, klasične grupe, specijalne grupe Liejevog tipa i sporadične grupe te ćemo spomenuti osnovno o njima. Također, spomenut ćemo i hrvatskog matematičara Zvonimira Janka, koji je zaslužan za veliko otkriće u familiji sporadičnih grupa.

Ključne riječi

Grupa, simetrična grupa, konačna grupa, jednostavna grupa, ciklička grupa, alternirajuća grupa, sporadična grupa, klasična grupa, specijalna grupa Liejevog tipa.

1 Uvod

Teorija grupa započinje svoj razvoj u 18. stoljeću sa Lagrangeom te osobito u 19. stoljeću zahvaljujući matematičarima Galoisu, Cauchyu, Abelu, Sylowu te Cayleyu koji je 1882. godine prvi detaljno proučavao konačne grupe. On je dokazao da se svaka konačna grupa može prikazati kao permutacijska grupa. Teorija grupa danas ima veliku primjenu u matematici i fizici. Grupe možemo podijeliti na konačne i beskonačne. Mi ćemo u ovom radu proučavati konačne grupe, a najviše ćemo se posvetiti konačnim jednostavnim grupama. Rad će se sastojati od uvođenja osnovnih pojmova koji su potrebni za razumijevanje konačnih jednostavnih grupa. Nakon toga, iskazat ćemo osnovni teorem o konačnim jednostavnim grupama te opisati pojmove koji se u njemu spominju.

2 Osnovni pojmovi

U ovom poglavlju navest ćemo osnovne pojmove, definicije i teoreme iz teorije grupa. Koristit ćemo [1] kao osnovnu literaturu u ovom poglavlju.

Definicija 2.1. *Neka je G neprazan skup. Svako preslikavanje $G \times G$ u skup G naziva se binarna operacija definirana na skupu G. Oznake: *, $\circ$, $\cdot$.*

Definicija 2.2. *Neka je G neprazan skup i neka je $*$ binarna operacija na skupu G za koju vrijedi $g_1 * g_2 \in G$, $\forall g_1, g_2 \in G$. Tada uređeni par $(G, *)$ zovemo grupoid.*

Definicija 2.3. *Asocijativni grupoid nazivamo polugrupa.*

Definicija 2.4. *Neka su $(G, \circ)$, $(H, *)$ grupoidi te neka je zadano preslikavanje $f : G \to H$. Kažemo da je f homomorfizam sa G u H ako $\forall a, b \in G$ vrijedi $f(a \circ b) = f(a) * f(b)$.*

Napomena 2.1. *Epimorfizam je surjektivni homomorfizam. Monomorfizam je injektivni homomorfizam. Izomorfizam je bijektivni homomorfizam.*

Definicija 2.5. *Uređeni par $(G, \circ)$ gdje je G neprazan skup, a $\circ$ binarna operacija na skupu G zovemo grupa ako vrijede sljedeća svojstva :*

1. $\forall a, b, c \in G$ *vrijedi* $a \circ (b \circ c) = (a \circ b) \circ c$,

2. $\exists e \in G$ *t.d. je* $a \circ e = e \circ a = a$, *za* $\forall a \in G$,

3. $\forall a \in G, \exists a' \in G$ *t.d je* $a \circ a' = a' \circ a = e$.

Ako za svaki $a, b \in G$ vrijedi $a \circ b = b \circ a$ tada kažemo da je $(G, \circ)$ komutativna ili Abelova grupa.

Definicija 2.6. *Red grupe G, koji se označava s $|G|$, je kardinalni broj grupe G.*

Definicija 2.7. *Red elementa a iz grupe G najmanji je pozitivan cijeli broj n takav da $a^n = e$, gdje je a^n umnožak [1] a sa samim sobom n puta. Ako ne postoji takav n, tada se kaže da je red od a beskonačan.*

Definicija 2.8. *Neka je G grupa i neka je H neprazan podskup od G. Kažemo da je H podgrupa od G ako je H grupa s obzirom na istu binarnu operaciju. Oznaka $H \leq G$.*

Primjer 2.1. *Neki primjeri grupa koji se spominju u [1] su:* $(\{0\}, +), (\{1\}, \cdot), (\mathbb{Z}, +)$

Definicija 2.9. *Bijektivna preslikavanja nepraznog skupa Ω na samoga sebe zovu se permutacije skupa Ω. Skup svih permutacija skupa Ω čini grupu koja se zove simetrična grupa na Ω.*

Napomena 2.2. *Neka je H podgrupa od G, $H \leq G$. Tada vrijede sljedeća svojstva:*

1. $\forall a, b \in H$ *mora vrijediti* $a \circ b \in H$, *tj.* $H \circ H \subseteq H$,
2. $1_G \in H$,
3. $a \in H \Rightarrow a^{-1} \in H$ *tj.* $H^{-1} \subseteq H$.

Primjer 2.2. *Primjer podgrupa:*

1. $G \leq G$
2. $1 \leq G$
3. *Prave netrivijalne podgrupe:* $1 < H < G$

U nastavku dajemo teorem koji daje kriterij za podgrupe.

Teorem 2.1. *Neka je G grupa, H neprazan podskup od G. H je podgrupa od G ako i samo ako $a \cdot b^{-1} \in H$ za sve $a, b \in H$.*

Dokaz. "$\Rightarrow$" $H \leq G \Rightarrow a, b \in H, \exists\, b^{-1} \in H \Rightarrow a \cdot b^{-1} \in H$

[1] umnožak u G će nam biti binarna operacija

"$\Leftarrow$" Pretpostavimo, $a, b \in H$ " $\Rightarrow$ " $a \cdot b^{-1} \in H$

Za H neprazan, $\exists a \in H$ " $\Rightarrow$ " $a \cdot a^{-1} \in H$ " $\Rightarrow$ " $1_G \in H$

Za $1, a \in H$ " $\Rightarrow$ " $1 \cdot a^{-1} \in H$ " $\Rightarrow$ " $a^{-1} \in H$

Za $a, b \in H$ " $\Rightarrow$ " $a, b^{-1} \in H$ " $\Rightarrow$ " $a \cdot (b^{-1})^{-1} \in H$ $\square$

Definicija 2.10. *Neka je G grupa i $S \subseteq G$. Najmanja podgrupa od G koja sadrži S označava se sa $< S >$ i zove se podgrupa koja generira podskup S. Elementi skupa S zovu se generatori (izvodnice) podgrupe S.*

Definicija 2.11. *Neka je G grupa i $a \in G$. Podgrupa $< a >$, $< a >= \{a^k : k \in \mathbb{Z}\}$ generirana elementom a zove se ciklička grupa generirana s a.*

Napomena 2.3. *Općenito, generator ne mora biti jedinstven.*

Definicija 2.12. *Neka je G grupa, $a \in G$. Ako $\exists m \in \mathbb{N}$ t.d je $a^m = e$, onda najmanji takav broj zovemo red elementa a i označavamo s $|a|$.*

U nastavku ćemo iskazati teorem koji opisuje redove elemenata. Dokaz se može pronaći u [1].

Teorem 2.2. *Neka je $G =< a >$, $H \leqslant G$. Tada je H ciklička grupa. Vrijedi: $H =< 1 >$ ili $H =< a^t >$, $t = min\{k : a^k \in H, k \in \mathbb{N}\}$.*
Ako je G konačna grupa, onda $|H| = \frac{|G|}{t}$.

Napomena 2.4. *Svaka grupa prostog reda je ciklička te svaka podgrupa cikličke grupe je ciklička. Svaka ciklička grupa je komutativna.*

3 Konačne grupe

3.1 Uvodno o konačnim grupama

Definicija 3.1. *Kažemo da je grupa G konačna ako je G konačan skup, a u suprotnom kažemo da je grupa G beskonačna.*

Primjer 3.1. *$(\mathbb{Z}_4, +)$ konačna je grupa čiji su elementi $\{0, 1, 2, 3\}$, a red te grupe je $|\mathbb{Z}_4| = 4$.*

Definicija 3.2. *Neka je H podgrupa od G. Definiramo desne klase od H kao $Hg = \{hg : h \in H\}$,a lijeve klase od H kao $gH = \{gh : h \in H\}$, gdje je $g \in G$.*

Dokaz sljedećeg teorema može se pronaći u [1].

Teorem 3.1. *Neka je G grupa, $H \leq G$. Lijeve klase grupe G po podgrupi H čine particiju od G. Analogno vrijedi i za desne klase grupe G po podgrupi H.*

Sve klase od H jednake su veličine, a taj rezultat korišten je u dokazu Lagrangeovog teorema, kojeg dajemo u nastavku.

Teorem 3.2. *Neka je G konačna grupa i $H \leqslant G$. Tada $|H| \mid |G|$.*

Dokaz. Dokazat ćemo da $\forall g \in G$ vrijedi $|gH| = |H|$. Definiramo funkciju $\rho : H \to gH, g \in G$, $\rho(h) = h\rho$. Vrijedi $H\rho = gH$ pa slijedi da je ρ surjekcija. Također vrijedi $h_1\rho = h_2\rho \Rightarrow gh_1 = gh_2 \Rightarrow h_1 = h_2$ pa je ρ injekcija. Kako je ρ injekcija i surjekcija, slijedi ρ je bijekcija pa $|gH| = |H|$. Prema prethodnom teoremu (Teorem 3.1), znamo da G/H čini particiju od G, pa $|G| = \sum{}_1{}^k |g_iH| = k \cdot H \Rightarrow |H|/|G|$. $\square$

Definicija 3.3. *Kažemo da je podgrupa N grupe G normalna u G i pišemo $N \trianglelefteq G$ ako su lijeve klase grupe G po podgrupi N ujedno i desne klase, tj. ako $\forall g \in G$ vrijedi $gN = Ng$*

Napomena 3.1. *U komutativnim (Abelovim) grupama sve podgrupe su normalne.*

Primjer 3.2. *Primjeri konačnih Abelovih grupa:*

1. $(\mathbb{Z}_4, +_4)$ *- ciklička Abelova grupa;*

2. *Podgrupe od* $(\mathbb{Z}_4, +_4)$*: I,* $(\mathbb{Z}_4, +)$, $(\mathbb{Z}_2, +)$ *su također konačne Abelove grupe.*

3.2 Sylowljeve podgrupe

Lagrangeov teorem (Teorem 3.2.) kaže nam da red bilo koje podgrupe od G dijeli red od G. U [8] navodi se sljedeći primjer koji pokazuje da obrat Lagrangeovog teorema ne vrijedi općenito.

Primjer 3.3. *Alternirajuća grupa A_4, $|A_4| = 12$ te vrijedi da 6 dijeli 12, ali A_4 nema podgrupu reda 6.*

L. Sylow pokazao je da obrat Lagrangeovog teorema ipak vrijedi u nekim slučajevima. Naime, on je pokazao da ako p^i dijeli $|G|$, gdje je p prost broj, tada G ima podgrupu reda p^i.

Definicija 3.4. *Neka je G konačna grupa i p prost broj. Tada vrijedi:*

1. *Grupa G zove se p-grupa ako je $|G| = p^k$ za neki prirodan broj k.*
2. *Podgrupa od G čiji red je p^i naziva se p-podgrupa od G.*
3. *Sylowljeva p-podgrupa od G (oznaka: Syl_pG) je odgrupa reda p^k, gdje je p^k najveća potencija od p koja dijeli $|G|$.*

Dokaz sljedeće propozicije može se pronaći u [5].

Propozicija 3.1. *Neka je G konačna Abelova grupa reda m i p prost broj, $p \mid m$. Tada G sadrži podgrupu reda p.*

U nastavku ćemo iskazati Sylowljeve teoreme. Dokazi se mogu naći u [1].

Teorem 3.3. *(Prvi Sylowljev teorem)*
Svaka konačna grupa G ima Sylowljeve p-podgrupe za svaki p prost broj.

Teorem 3.4. *(Drugi Sylowljev teorem)*
Sve su Sylowljeve p-podgrupe od G međusobno konjugirane podgrupe od G. Svaka je p-podgrupa od G sadržana u nekoj Sylowljevoj p-podgrupi od G, gdje je p prost broj.

Teorem 3.5. *(Treći Sylowljev teorem)*
Broj Sylowljevih p-podgrupa konačne grupe G kongruentan je sa 1 mod p, tj.

$$|Syl_pG| \equiv 1 (mod p).$$

Primjer 3.4. *U [8] dani su sljedeći primjeri Sylowljevih podgrupa:*

1. *Grupa $\mathbb{Z}_{12}$ reda $12 = 2^2 \cdot 3$ ima jednu Sylowljevu 3-podgrupu reda 3 $\{0, 4, 8\}$ i jednu Sylowljevu 2-podgrupu reda 4 $\{0, 3, 6, 9\}$.*
2. *Simetrična grupa S_3 reda $6 = 2^2 \cdot 3$ ima jednu Sylowljevu 3-podgrupu $\{(1), (123), (132)\}$ i tri Sylowljeve 2-podgrupe $\{(1), (12)\}$, $\{(1), (23)\}$, $\{(1), (13)\}$.*

4 Klasifikacija konačnih jednostavnih grupa

4.1 Jednostavne grupe

Definicija 4.1. *Grupa je jednostavna ako nema pravih netrivijalnih normalnih podgrupa.*

Napomena 4.1. *Sve konačne grupe prostog reda su jednostavne te su to ujedno i jedine (konačne) komutativne jednostavne grupe. Najmanje nekomutativne jednostavne grupe su reda 60 (grupa A_5) i 168 (grupa $GL(3,2)$).*

Definicija 4.2. *Neka je G konačna grupa. Normalni niz grupe G je strogo padajući niz podgrupa $G = G_0 \trianglelefteq G_1 \trianglelefteq G_2 ... \trianglelefteq G_n = 1$.*

Definicija 4.3. *Ako se među susjednim članovima ne mogu ubaciti nove grupe i ujedno očuvati uvjeti niza tada se normalni niz zove se kompozicijski niz grupe G.*

Definicija 4.4. *Kompozicijske grupe su faktorske grupe G_{i-1}/G_i, $i = 1, 2, ..., n$.*

Motivacija za klasifikaciju grupa potječe iz Jordan-Hölderovog teorema čiji iskaz dajemo u nastavku, a dokaz se može pronaći u [11].

Teorem 4.1. *Svi kompozicijski nizovi grupe G imaju jednaku duljinu i do na permutaciju izomorfne kompozicijske faktore.*

Napomena 4.2. *Stvaranje kompozicijskih nizova slično je faktoriziranju prirodnih brojeva u njegove prim faktore. Analogno, svi prirodni brojevi su građeni od prim brojeva i sve konačne grupe građene su od konačnih jednostavnih grupa.*

4.2 Teorem o klasifikaciji konačnih jednostavnih grupa

Klasifikacija konačnih jednostavnih grupa dovršena je 1981. godine, a predstavlja jednu od najistaknutijih postignuća u povijesti matematike. Postoji izniman broj istraživačkih radova uključenih u rješenje. Na dokazu teorema o klasifikaciji konačnih jednostavnih grupa radilo stotine matematičara diljem svijeta u razdoblju od 30 godina, a puni dokaz ima između 5000 i 10000 stranica časopisa.

U nastavku ćemo iskazati glavni teorem o klasifikaciji konačnih jednostavnih grupa, a dokazi dijelova tog teorema mogu se pronaći u [6].

Teorem 4.2. *Svaka konačna jednostavna grupa izomorfna je jednoj od sljedećih grupa:*

1. *cikličkoj grupi prostog reda,*
2. *alternirajućoj grupi, A_n, $n \geq 5$,*
3. *klasičnoj grupi,*

4. *specijalnoj grupi Liejevog tipa,*

5. *jednoj od 26 sporadičnih jednostavnih grupa.*

U nastavku ćemo opisati svaku grupu iz prethodnog teorema.

4.2.1 Cikličke grupe prostog reda

Teorem 4.3. *Neka je G konačna grupa reda $|G| \geq 2$ i neka je $a \in G$, $a \neq G$. Tada $|a|$ dijeli $|G|$. Nadalje, ako je $|G|$ prosti broj, onda je G ciklička grupa.*

Napomena 4.3. *Budući da cikličke grupe $\mathbb{Z}_p$, za p prost broj nemaju prave netrivijalne normalne podgrupe, tada su sve te grupe primjeri jednostavnih grupa.*

4.2.2 Alternirajuće grupe, A_n, $n \geq 5$

Neka je S neprazan skup. Permutacija skupa bijekcija je sa S na S. Ako je $|S| = n$, onda se grupa permutacija skupa S naziva simetrična grupa n-tog reda i označava sa S_n. Permutacije koje neke elemente skupa S ciklički rotiraju nazivaju se cikličke permutacije.

Definicija 4.5. *Grupa G djeluje na konačan skup Ω ako postoji preslikavanje $f : G \times \Omega \to \Omega$ takvo da vrijedi:*

1. $f(g_1, f(g_2, x)) = f(g_1 g_2, x), \forall x \in \Omega,\ \forall g_1, g_2 \in G,$

2. $f(1, x) = x, \forall x \in \Omega.$

Slika djelovanja elementa $g \in G$ na element $x \in \Omega$ označava se sa $g.x$ ili x^g.

Definicija 4.6. *Skup $G_x = \{g \in G : g.x = x\} \leq G$ naziva se stabilizator elementa x za djelovanje grupe G.*

Dokaz sljedećeg korolara može se pronaći u [3].

Korolar 4.1. *Svaka permutacija može se zapisati kao umnožak transpozicija.*

Definicija 4.7. *Kažemo da je permutacija $\sigma \in S_n$ parna (neparna), ako se može zapisati kao umnožak parnog (neparnog) broja transpozicija. Permutacija ima pozitivan predznak ako je permutacija parna, a negativan predznak ako je permutacija neparna.*

Definicija 4.8. *Alternirajuća grupa je konačna grupa parnih permutacija definirana na konačnom skupu $\{1, 2, ..., n\}$. Red alternirajuće grupe je $\frac{n!}{2}$.*

Dokaz sljedeće propozicije može se pronaći u [6].

Propozicija 4.1. *Ako je $n \geq 7$ i $A_{n-1} \cong H \leq A_n$, tada je H stabilizator jedne od n točaka na koje A_n djeluje.*

Teorem 4.4. *Ako je $n \leq 7$ tada je $Aut(A_n) \cong S_n$.*

Dokaz teorema može se pronaći u [5], a teorem vrijedi također za $n = 4$ i $n = 5$.

Napomena 4.4. *Podgrupa H u grupi G je normalna, ako se sastoji od unije konjugiranih klasa u G.*

Lagrangeov teorem nam kaže da je svaka grupa prostog reda jednostavna i to vrijedi jer grupa prostog reda nema netrivijalnih normalnih podgrupa, dok alternirajuće grupe imaju mnoštvo podgrupa pa su tako zanimljiviji primjeri jednostavih grupa. U nastavku ćemo ukratko opisati alternirajuće grupe A_n, $n \in \{1, 2, 3, 4\}$ te navesti teorem koji nam kaže koje alternirajuće grupe su jednostavne.
Alternirajuća grupa A_2 je trivijalna. Alternirajuća grupa A_3 je jednostavna. Alternirajuća grupa A_4 nije jednostavna grupa jer je $K = \{Id, (12)(34), (13)(24), (14)(23)\}$ netrivijalna podgrupa u simetričnoj grupi S_4. Kako je $K < A_4$ slijedi da alternirajuća grupa A_4 nije jednostavna. U nastavku ćemo pokazati da je alternirajuća grupa A_5 jednostavna.

Teorem 4.5. *Alternirajuća grupa A_5 je jednostavna grupa.*

Dokaz. Alternirajuća grupa A_5 ima pet konjugacijskih klasa koje imaju redom 1, 20, 15 i 12 elemenata (postoje dvije klase s 12 elemenata). Kako nema odgovarajućeg zbroja tih brojeva koji dijeli broj 60, a to nam je broj elemenata alternirajuće grupe A_5, slijedi da nema niti podgrupe koja se može dobiti kao unija konjugacijskih klasa, pa je prema Napomeni 4.4. A_5 jednostavna grupa. $\square$

Induktivno možemo pokazati da tvrdnja prethodnog teorema vrijedi za svaki $n \geq 5$, a dokaz toga može se pronaći u [6].

Teorem 4.6. *Alternirajuća grupa A_n je jednostavna za svaki $n \geq 5$.*

4.2.3 Klasične grupe

Sve klasične grupe definirane su u terminima grupa matrica nad poljima pa prije nego što krenemo proučavati konačne klasične grupe moramo znati što su konačna polja.

Definicija 4.9. *Polje je uređena trojka* $(\mathbb{F}, +, \cdot)$ *pri čemu je* F *neprazan skup, a operacije* $+$ *i* $\cdot$ *su binarne operacije na skupu sa svojstvima:*

1. $(\mathbb{F}, +)$ *je komutativna grupa,*
2. $(\mathbb{F}, \cdot)$ *je komutativna grupa,*
3. $\forall a, b, c \in \mathbb{F}$ *vrijedi* $(a + b) \cdot c = a \cdot c + b \cdot c$.

Definicija 4.10. *Determinanta je homomorfizam iz multiplikativne grupe svih regularnih matrica istog reda u multiplikativnu grupu* $\mathbb{R}\backslash\{0\}$.

Definicija 4.11. *Jezgra determinante, tj.* $det^{-1}(1)$ *je skup svih kvadratnih matrica reda* n *determinante 1.*

Neka je V *vektorski prostor dimenzije* n *nad konačnim poljem* $\mathbb{F}_q$ *reda* q. *Opća linearna grupa* $GL(V)$ *je skup invertibilnih linearnih preslikavanja sa skupa* V *na samog sebe. Bez smanjenja općenitosti možemo uzeti da je* V *kao vektorski prostor u polju* $\mathbb{F}_q$ *i identificirati* $GL(V)$ *s grupom invertibilnih* $n \times n$ *matrica nad* $\mathbb{F}_q$. *Postoje određene očite normalne podgrupe od* $G = GL_n(q)$. *Na primjer, centar* Z *sastoji se od svih skalarnih matrica* λI_n, *gdje je* $0 \neq \lambda \in \mathbb{F}$ *i* I *je* $n \times n$ *matrica identiteta. Stoga je* Z *ciklička normalna podgrupa reda* $q - 1$. *Kvocijent* $G \setminus Z$ *naziva se projektivna opća linearna grupa i označava se sa* $PGLn(q)$.

Postoji točno 6 familija klasičnih jednostavnih grupa. To su:

1. linearna : $PSL_n(q)$, $n \geq 2$, osim $PSL_2(2)$ i $PSL_2(3)$,
2. unitarna : $PSU_n(q)$, $n \geq 3$, osim $PSU_3(2)$,
3. simplektička: $PS_{P2n}(2)$, $n \geq 2$, osim $PS_{P4}(2)$,
4. tri familije ortogonalnih grupa, a to su:
   (a) $P\Omega_{2n+1}(q)$, $n \geq 3$, q neparan,
   (b) $P\Omega^{+}{}_{2n}(q)$, $n \geq 4$,
   (c) $P\Omega^{-}{}_{2n}(q)$, $n \geq 4$,

   gdje je q potencija prostog broja p.

U nastavku ćemo opisati redove tih klasičnih konačnih jednostavnih grupa.

Redovi linearnih klasičnih konačnih jednostavnih grupa, $PSL_n(q), n \geq 2$

Neka je V vektorski prostor nad poljem $\mathbb{F}_q$ reda q. Grupu invertibilnih $n \times n$ matrica zovemo opća linearna grupa i označavamo sa $Gl_n(q)$. Red opće linearne grupe jednak je $|Gl_n(q)| = (q^n - 1)(q^n - q^2) \cdots (q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}}(q-1)(q^2-1) \cdots (q^n - 1)$. Redovi od $SL_n(q)$ i $PGL_n(q)$ su jednaki, a njihov red jednak je $|Gl_n(q)|$ podijeljeno sa $q - 1$. Da bismo dobili red od $PSL_n(q)$, moramo znati koji skalari λI_n imaju determinantu 1. Vrijedi $det(\lambda In) = \lambda^n$, a broj rješenja za $\lambda^n = 1$ u polju $\mathbb{F}_q$ je najveći zajednički djeljitelj od n i $q-1$, $(n, q-1)$. Dakle, red od $PSLn(q)$ je $|PSLn(q)| = \frac{1}{(n,q-1)} g^{\frac{n(n-1)}{2}} \prod_2^n (q^i - 1)$.

Redovi slimplektičkih konačnih jednostavnih grupa, $PSU_n(q)$**,** $n \geq 3$

Simplektična grupa $S_{P_{2m}}(g)$ izomorfna je podgrupi $GL_{2m}(q)$ koja se sastoji od elemenata q za koje vrijedi $f(u^q, v^q) = f(u,v), \forall u, v \in V$. Prostor V ima simplektičku bazu $\{e_1, ..., e_m, f_1, ..., f_m\}$ za koju vrijedi da su svi vektori baze međusobno okomiti jedni na druge, osim $f(e_i, f_i) = 1$. Da bismo izračunali red simplektičke grupe moramo prebrojiti načine na koje možemo odabrati vektore baze. Vektor e_1 može biti bilo koji nenul vektor pa možemo birati na q^{2m-1} načina. Tada je vektor ortogonalni na e_1 dimenzije $2m-1$ pa sadrži q^{2m-1} vektora. Sada postoje $q^{2m} - q^{2m-1} = (q-1)q^{2m-1}$ vektora v t.d. $f(u,v) \neq 0$. Također, vektor f_1 možemo odabrati na q^{2m-1} načina. Stoga indukcijom dolazimo do reda od $S_{P_{2m}}(g)$, $|S_{P_{2m}}(g)| = \prod(q^{2i}-1)q^{2i-1} = q^{m^2} \prod(q^{2i}-1), i \in \{1, 2, ..., m\}$. Primjetimo da je $f(\lambda u, \lambda v) = \lambda^2 f(u,v)$ jednak $f(u,v)$ ako i samo ako vrijedi $\lambda = \pm 1$. Grupa $PS_{P_{2m}}(g)$ definirana je kao kvocijent od $S_{P_{2m}}(g)$ po podgrupama kvadratne matrice.

Redovi ortogonalnih konačnih jednostavnih grupa

Mnoge su ortogonalne grupe izomorfne drugim klasičnim grupama, a redovi tih ortogonalnih grupa jednaki su redu izomorfne grupe. U nastavku ćemo navesti neke od izomorfizama:

$P\Omega_3(q) \cong PSL_2(q)$, $P\Omega_4{}^+(q) \cong PSL_2(q) \times PSL_2(q)$, $P\Omega_4{}^-(q) \cong PSL_2(q^2)$, $P\Omega_5(q) \cong PSL_{p_4}(q)$, $P\Omega_6{}^+(q) \cong PSL_4(q)$,$P\Omega_6{}^-(q) \cong PSU_4(q)$.

Više o ovim grupama, može se pronaći u [6].

4.2.4 Specijalne grupe Liejevog tipa

U ovom dijelu navest ćemo 10 familija takozvanih specijalnih grupa Liejevog tipa. Postoje tri glavna pristupa tim grupama. Prvi je pomoću Liejevih algebri koji nam omogućava konstrukciju jednostavnih grupa, drugi, moderniji pristup je pomoću algebarskih grupa. Treći pristup je pomoću alternirajućih algebri koji dobiva značajnu prednost kada je u pitanju izvođenje konkretnih proračuna. Sa stajališta Liejevih algebri, tri su različita tipova specijalnih grupa. Najjednostavnije su Chevalleyeve grupe $G_2(g)$, $F_4(q)$, $E_n(q)$ za $n = 6, 7, 8$. Sljedeće po redu su Steinberg-Tits-Hertzig uvrnute (engl. twisted) grupe $D_4(q)$, $E_6(q)$ koje postoje za svako konačno polje $\mathbb{F}_q$ i čije su konstrukcije analogne konstrukcijama unitarnih grupa iz klasičnih grupa. Treći tip grupa su Suzuki-Ree grupe $B_2(2^{2n+1}) = S_z(2^{2n+1})$, $G_2(3^{2n+1}) = R(3^{2n+1})$, $F_4(2^{2n+1}) = R(2^{2n+1})$, za $n \geq 1$. Više o tim grupama može se pronaći u [6].

4.2.5 Jednostavne sporadične grupe

Prve sporadične grupe otkrio je Emile Mathieu 1860-ih, kada je pronašao pet takvih grupa. Godine 1965., nakon gotovo više od stoljeća, Zvonimir Janko pronašao je grupu J_1 reda 175560. Tijekom sljedećih 10 godina otkriveno je još 20 sporadičnih grupa. Najveću sporadičnu grupu pod nazivom Monster grupe (engl. Monster group) veličine $8.08 \cdot 10^{53}$ otkrili su Bernd Fischer i Robert Griess. Sporadične grupe možemo podijeliti u dvije skupine. Prvu skupinu pod nazivom engl. Happy Family čini 20 podgrupa Monster grupe, dok preostalih 6 spada u skupinu pod nazivom Paraih grupe (engl. Paraih groups). Prije nego što opišemo te grupe, pojasnit ćemo pojam tranzitivnosti.

Definicija 4.12. *Neka je G grupa i $\rho : G \to S(\Omega)$, $|\Omega| = n$, ρ je homomorfizam sa G u $S(\Omega)$. Tada se ρ zove permutacijska reprezentacija grupe G na skupu Ω.*

Definicija 4.13. *Kažemo da je ρ permutacijska reprezentacija stupnja n. Kažemo da je reprezentacija vjerna ako je ρ homomorfizam koji je injektivan.*

Ekvivalentno, kažemo da grupa G djeluje na skup Ω.

Definicija 4.14. *Neka grupa G djeluje na skupu Ω, $\alpha, \beta \in \Omega$ su G-povezani ako $\exists g \in G$ tako da $\alpha g = \beta$.*

Definicija 4.15. *Klase ekvivalencije G-povezanosti zovu se G-orbite na skupu Ω i pišemo*

$\alpha^G = \{\alpha g : g \in G\}$.

Definicija 4.16. *Grupa G djeluje tranzitivno na skupu Ω ako ima samo jednu orbitu, tj. ako je $\alpha^G = \Omega$, za svaki $\alpha \in \Omega$.*

Definicija 4.17. *Djelovanje grupe G je slobodno ako $\forall s \in \Omega$, $gs = s$ implicira $g = e_G$.*

Definicija 4.18. *Grupa G je strogo (engl. sharply) tranzitivna, ako je tranzitivna i slobodna.*

Prvu skupinu sporadičnih grupa pod nazivom Happy Family, podijelit ćemo u tri generacije.

Prva generacija: Mathieuove grupe

Otkriće najranijih sporadičnih grupa u razdoblju od 1861. do 1873. pripisuje se Emileu Leonardu Mathieu. On se zanimao za višestruko tranzitivne permutacijske grupe pa su tako nastale Mathieuove čije redove i tranzitivnost možete vidjeti u Tablici 1.

Tablica 1: Prva generacija: Mathieuove grupe

Grupa	Red	Tranzitivnost
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	4-tranzitivna (strogo)
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	5-tranzitivna(strogo)
M_{21}	$2^6 \cdot 3^2 \cdot 5 \cdot 7$	2-tranzitivnost
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	3-tranzitivnost
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	4-tranzitivnost
M_{24}	$2^10 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	5-tranzitivnost

Druga generacija: Leech Lattice

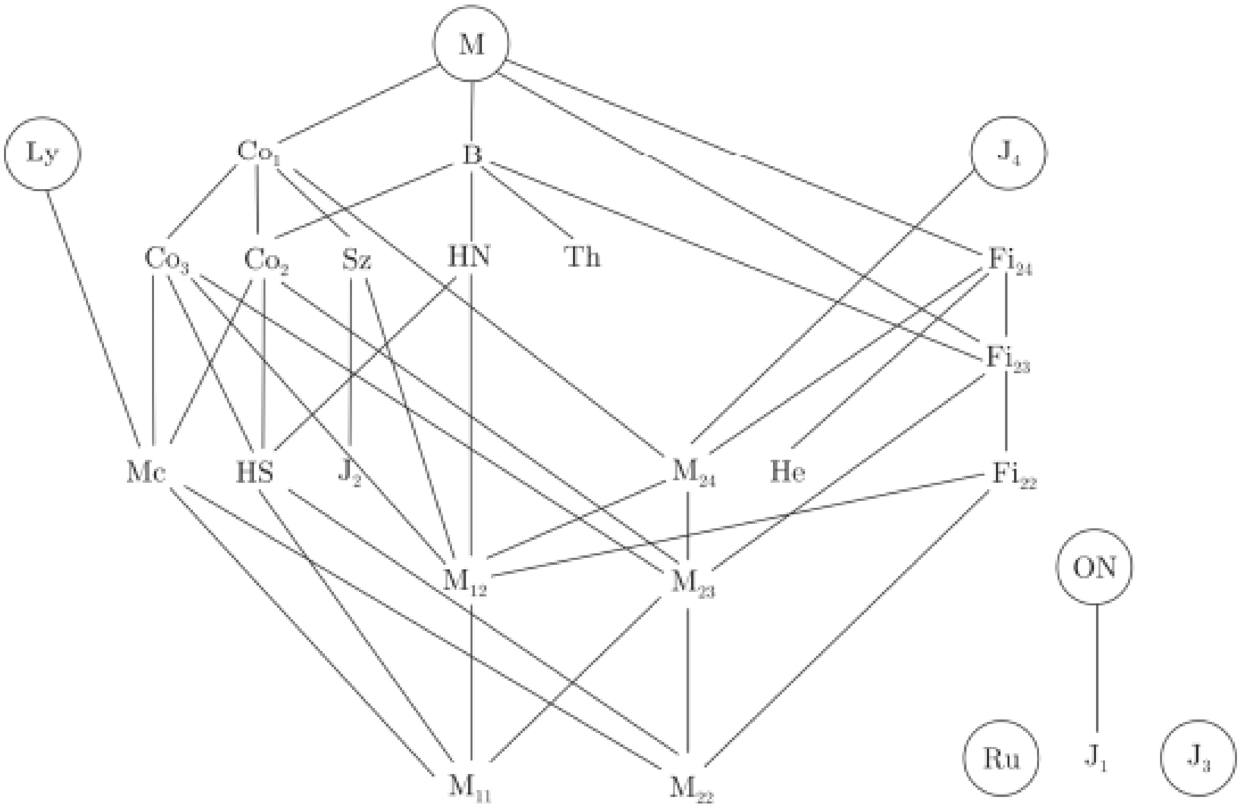
Grupu Leech Lattice A_{24} otkrio je John Leech 1967. godine kada je radio na problemu engl. Kissing number problem. John Conway 1968. otkrio je da je grupa automorfizama Leechove rešetke grupa reda $|Aut(A_{24})| \equiv |Co_0| = 2^2 \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$. Iako grupa Co_0 nije jednostavna, ona ima jednostavne podgrupe koje tvore sporadične grupe. U Tablici 2 navedene su sporadične grupe druge generacije.

Tablica 2: Leech Lattice grupe

Grupa	Red
Co_1 (*Conway*)	$2^{31} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
Co_2(*Conway*)	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Co_3(*Conway*)	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
HS (*Higman-Sims*)	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
HJ ili J_2 (*Hall-Janko*)	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
Suz (*Suzuki*)	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7$

Treća generacija: Monster grupe

Grupa Monster M najveća je sporadična grupa i povezana je s 20 od ukupno 26 sporadičnih grupa. Povezanost Monster grupe sa ostalim sporadičnim grupama prikazana je na Slici 1.



Slika 1: Veza između sporadičnih grupa (preuzeto iz [2]).

Matematičari Bernd Fischer i Robert Griess zaslužni su za konstrukciju Monstera koji je bio dovršen 1982. godine, stoga je ta grupa poznata kao Fischer-Griessovo čudoviste. Fischer je također otkrio Baby Monster B i još tri sporadične grupe Fi_{22},Fi_{23} i Fi_{24}. U Tablici 3 nalaze se sporadične grupe treće generacije i njihovi redovi.

Tablica 3: Treća generacija: Monster grupe

Grupa	Red
M $(Monster)$	$\approx 8 \cdot 10^{54}$
B $(BabyMonster)$	$\approx 8 \cdot 4^{33}$
Fi_{24} $(Fischer)$	$\approx 1 \cdot 10^{24}$
Fi_{23} $(Fischer)$	$\approx 4 \cdot 10^{18}$
Fi_{22} $(Fischer)$	$\approx 6 \cdot 10^{13}$
HN $(Harda\text{-}Norton)$	$\approx 2 \cdot 10^{14}$
Th $(Thompson)$	$\approx 9 \cdot 10^{17}$
He $(Held)$	$\approx 4 \cdot 10^{9}$

Pariahove grupe

Kod grupa treće generacije spomenuli smo kako je Monster grupa povezana s 20 od ukupno 26 sporadičnih grupa, a preostalih 6 sporadičnih grupa koje nisu povezane s Monster grupom spadaju u Pariahove grupe te su navedene u tablici ispod (Tablica 4).

Tablica 4: Pariahove grupe

Grupa	Red
Ru $(Rudvalis)$	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
ON $(O'Nan)$	$2^{9} \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
Ly $(Lyons)$	$2^{8} \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
J_4 $(Janko)$	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
J_3 $(Janko)$	$2^{7} \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
J_1 $(Janko)$	$2^{3} \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$

Veliki doprinos u otkriću nekih sporadičnih grupa ima i hrvatski matematičar Zvonimir Janko.

4.2.6 Zvonimir Janko

Hrvatski matematičar Zvonimir Janko, rođen je u Bjelovaru 1932. godine. Bavio se proučavanjem teorije konačnih grupa, a posebno se posvetio klasifikaciji konačnih jednostavnih grupa te 1964. godine dolazi do velikog otkrića - prve Jankove sporadične jednostavne grupe J_1. To otkriće izazvalo je mnoga pitanja jer se smatralo da postoji samo pet Mathieuovih sporadičnih jednostavih grupa. Došlo je do pitanja ima li sporadičnih grupa beskonačno mnogo te hoće li se ikada moći sve klasificirati. Tada je počelo istraživanje koje je trajalo oko 30 godina i na kojem je sudjelovalo više od 100 teoretičara grupa koji su na kraju dokazali potpunu klasifikaciju svih konačnih jednostavnih grupa, a dokaz je zahtjevao 10 000 stranica časopisa. Bio je to jedan od rijetkih ključnih matematičkih problema koji je do kraja riješen. Od 21 grupe koje su se otkrile nakon prve Jankove grupe, profesor Janko otkrio je četiri, to su J_1, J_2, J_3, J_4.

Slika 2: Zvonimir Janko (preuzeto iz [9]).

Zaključak

Cilj ovog rada bio je klasificirati konačne jednostavne grupe. Rad se sastoji od uvođenja osnovnih pojmova koji su potrebni za razumijevanje konačnih jednostavnih grupa, zatim je iskazan osnovni teorem o konačnim jednostavnim grupama pomoću kojeg smo klasificirali konačne jednostavne grupe na cikličke grupe prostog reda, alternirajuće grupe, klasične grupe, specijalne grupe Liejevog tipa te sporadične jednostavne grupe. Dokaz teorema o klasifikaciji konačnih jednostavnih grupa jedno je od najznačajnijih postignuća u povijesti matematike. Na dokazu je radilo nekoliko stotina matematičara diljem svijeta u razdoblju od 30 godina, a puni dokaz ima između 5000 i 10000 stranica časopisa. U radu je ukratko opisana svaka grupa iz teorema. Spomenuli smo i hrvatskog matematičara koji je imao iznimnu važnost u teoriji sporadičnih grupa.

Literatura

[1] Bilješke s predavanja iz kolegija Algebarske strukture, nositelj: Andrea Švob, akademska godina 2021./2022.

[2] G. Sheng: On the Classification of Finite Simple Groups, 2022.
URL:https://math.mit.edu/research/highschool/primes/circle/documents/2022/Gracie.pdf (16.6.2023.)

[3] H. Kraljević: Algebra, predavanja održana na Odjelu za matematiku Sveučilista Josipa Jurja Strossmayera u Osijeku u ljetnom semestru akademske godine 2006./2007.
URL: https://web.math.pmf.unizg.hr/~hrk/nastava/2006-07/algebra_Osijek_2006_7.pdf (25.3.2023.)

[4] J. D. Dixon, B. Mortimer, Permutation Groups, Springer, 1996.

[5] N. Grbac, V. Mikulić Crnković: Algebarske strukture, prva verzija skripte, 2010/2011
URL: https://www.math.uniri.hr/~ngrbac/alg_str_web.pdf (01.3.2023.)

[6] R.A. Wilson: The Finite Simple Groups, Springer, London, 2009.

[7] R.C. Daileda: The Alternating Group URL:http://ramanujan.math.trinity.edu/rdaileda/teach/s19/m3362/alternating.pdf(26.4.2023.)

[8] S. Krešic-Jurić: Algebarske strukture, Skripta, 2013. URL:https://mapmf.pmfst.unist.hr/~skresic/Algebra/Skripta/Algebarske_strukture_v4.pdf (25.3.2023.)

[9] Supplement. Finite Simple Groups, 2014
URL: https://faculty.etsu.edu/gardnerr/4127/notes/Simple-Groups.pdf (28.2.2023.)

[10] V. Ćepulić: Profesor Zvonimir Janko i teorija grupa, 2007.
URL: https://www.croatianhistory.net/etf/janko/janko_cepulic.html (08.03.2023.)

[11] W. Kochanski: The Jordan Holder Theorem
URL: https://www.math.brown.edu/dabramov/MA/f1516/251/JordanHolder.pdf (22.3.2023.)