Slobodne grupe i prezentacije

Čukec, Petra

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Petra Čukec

SLOBODNE GRUPE I PREZENTACIJE

Diplomski rad

Voditelj rada:
Prof. dr. sc. Dražen Adamović

Zagreb, rujan 2015

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Uvod

Teorija grupa je dio algebre koji proučava strukturu grupa, njihove reprezentacije te klasifikaciju grupa. Pojam grupe je središnji pojam apstraktne algebre koji se sastoji od skupa i binarne operacije koja spaja dva elementa tog skupa te iz njih formira treći iste vrste. Pritom operacija mora zadovoljavati aksiome grupe.

Osnovni pojmovi koje proučavamo u ovom radu su slobodne grupe i prezentacije:

Definicija 1. *Neka je X podskup grupe F. Kažemo da je F* ***slobodna grupa s bazom*** *X ako za svaku grupu G i svaku funkciju $f : X \to G$ postoji jedinstveni homomorfizam $\overline{f} : F \to G$ takav da vrijedi: $\overline{f}(x) = f(x)$, $\forall x \in X$.*

Definicija 2. *Neka je X skup, $F = F(X)$ slobodna grupa s bazom X i $R \subseteq F$ skup riječi nad X. Grupa G ima* ***prezentaciju*** *$G = (X \mid R)$ ako je $G \cong F/N$, pri čemu je N normalna podgrupa od F generirana sa R, odnosno N je najmanja normalna podgrupa od F koja sadrži R.*

Objasnimo sada detaljnije strukturu rada. Rad se sastoji od šest poglavlja. Prvo poglavlje sastoji se od uvodnih definicija i pojmova čije poznavanje će nam biti potrebno za kasnije razumijevanje sadržaja. Tu će biti definirani najvažniji pojmovi vezani za grupe kao i neka bitnija preslikavanja među njima.

U drugom poglavlju detaljnije ćemo se osvrnuti na pojam kategorije koji će nam u idućem poglavlju biti potreban pri konstrukciji slobodne grupe.

Definicija 3. ***Kategorija*** $\mathcal{C}$ *je klasa objekata koje označavamo sa* $(A, B, C, \ldots)$ *zajedno sa:*

(i) *klasom disjunktnih skupova za svaki par objekata iz* $\mathcal{C}$ *koju označavamo sa* $hom(A, B)$*. Elemente* $f \in hom(A, B)$ *nazivamo* ***morfizmi*** *iz* A *u* B *i označavamo sa* $f : A \to B$*.*

(ii) *funkcijom za svaku trojku* (A, B, C) *objekata od* $\mathcal{C}$ *:*

$$hom(B, C) \times hom(A, B) \to hom(A, C)$$

Za morfizme $f : A \to B$ *i* $g : B \to C$ *ovu funkciju možemo zapisati na sljedeći način:* $(g, f) \longmapsto g \circ f$ *i pritom* $g \circ f : A \to C$ *nazivamo* ***kompozicija*** *od* f *i* g*.*

Pritom moraju biti zadovoljeni aksiomi asocijativnosti i identitete.

Uz definiciju, navest ćemo i četiri primjera kategorija - kategoriju skupova $\mathcal{S}$, grupa $\mathcal{G}$, Abelovih grupa $\mathcal{A}$ i komutativnih prstena $\mathcal{R}$. Nakon toga, definirat ćemo pojam konkretne kategorije.

Definicija 4. *Neka je objekt* $A \in \mathcal{C}$*.* ***Konkretna kategorija*** *je kategorija* $\mathcal{C}$ *zajedno sa funkcijom* σ *koja svakom* A *pridružuje skup* $\sigma(A)$*. Pritom* $\sigma(A)$ *nazivamo* ***pripadni skup*** *od* A*. On ima sljedeća svojstva:*

1. *Svaki morfizam* $A \to B$ *iz* $\mathcal{C}$ *je funkcija na pripadnim skupovima* $\sigma(A) \to \sigma(B)$*.*
2. *Morfizam* $1_A : A \to A$ *je funkcija identite* $I_{\sigma(A)} : \sigma(A) \to \sigma(A)$*.*
3. *Kompozicija morfizama je kompozicija funkcija na pripadajućim skupovima.*

U konkretnoj kategoriji grupa $\mathcal{G}$ definirat ćemo slobodni objekt nad nepraznim skupom X.

Definicija 5. *Neka je F objekt u konkretnoj kategoriji $\mathcal{C}$, X neprazan skup i $i : X \to F$ preslikavanje između skupova. Kažemo da je F* ***slobodan nad skupom*** *X ako za svaki objekt $A \in \mathcal{C}$ i za svaki $f : X \to A$ postoji jedinstveni morfizam $\overline{f} : F \to A$ takav da vrijedi: $\overline{f} \circ i = f$.*

Zatim ćemo taj isti objekt proučavati u kategoriji grupa $\mathcal{G}$ što nas dovodi do definicije slobodne grupe (Definicija 1). Na isti način se može definirati i slobodna Abelova grupa kao slobodni objekt nad skupom X u kategoriji Abelovih grupa.

Postupak konstrukcije slobodne grupe F tema je idućeg poglavlja. Prije svega, definirat ćemo pojmove koji će nam biti potrebni kod konstrukcije. Ključni pojam je pojam riječ.

Definicija 6. *Neka je X skup koji nazivamo* ***abeceda****. Ako je n pozitivan broj,* ***riječ w*** *nad X duljine $n \geq 1$ je funkcija $w : \{1, 2, \ldots, n\} \to X$. Duljinu riječi w označimo sa $|w| = n$. Neka je 1 simbol koji nije sadržan u X. Njega nazivamo* ***praznom riječju*** *odnosno riječ duljine 0.*

Uz to, definirat ćemo inverz neprazne riječi, podriječ te reduciranu riječ. Nakon što pokažemo da je binarna operacija $u * v = red(uv)$ dobro definirana operacija na skupu $F(X)$, dokazat ćemo i teorem koji nam osigurava egzistenciju slobodne grupe.

Teorem 7. *Ako je X skup, $F(X)$ je skup svih reduciranih riječi na X. Skup $F(X)$ sa binarnom operacijom $u * v = red(uv)$ je* ***slobodna grupa*** *sa bazom X.*

Tema četvrtog poglavlja su slobodne Abelove grupe. Uz njihovu definiciju, definirat ćemo i rang slobodne Abelove grupe te pokazati da on ne ovisi o izboru baze. Zatim ćemo pokazati da je slobodna Abelova grupa slobodan objekt u kategoriji Abelovih grupa.

Teorem 8. *Neka je F slobodna Abelova grupa sa bazom $X = x_1, \ldots, x_n$. Za svaku Abelovu grupu G i za svaku funkciju $\gamma : X \to G$ postoji jedinstveni homomorfizam $h : F \to G$ takav da vrijedi: $h(x_i) = \gamma(x_i)$, $\forall x_i$.*

Na kraju poglavlja definirat ćemo pojam komutatora za dva elementa grupe i komutatorsku podgrupu te dokazati teorem koji daje vezu između tih definicija i slobodnih Abelovih grupa.
Pojmovi i tvrdnje iz četvrtog poglavlja podloga su za iduće poglavlje u kojem će biti riječi o rangu slobodne grupe. Uz definiciju, dokazat ćemo i sljedeći teorem.

Teorem 9. *Neka je F slobodna grupa s bazom X i G slobodna grupa sa bazom Y. Tada vrijedi: $F \cong G \Leftrightarrow |X| = |Y|$.*

Tema posljednjeg šestog poglavlja su prezentacije (Definicija 2). Nakon definicije i nekoliko primjera, definirat ćemo tip grupe.

Definicija 10. *Grupa G je **tipa** $\mathbb{T}(x, y \mid x^{2^{n-1}}, yxy^{-1}x, y^{-2}x^{2^{n-2}})$ ako je $n \geq 2$ i G je generirana sa dva elementa a i b takva da vrijedi: $a^{2^{n-1}} = 1$, $bab^{-1} = a^{-1} \quad i \quad b^2 = a^{2^{n-2}}$.*

Tip grupe povezat ćemo sa prezentacijama preko *von Dyck-ovog teorema*.

Teorem 11. ***(von Dyck-ov teorem)***

(i) *Ako grupe G i H imaju prezentacije: $G = (X \mid R) \quad i \quad H = (X \mid R \cup S)$, tada je H kvocijent od G. Posebno, ako je H grupa tipa $\mathbb{T}(X \mid R)$, tada je H kvocijent od G.*

(ii) *Neka je $G = (X \mid R)$ i neka je H grupa tipa $\mathbb{T}(X \mid R)$. Ako je G konačna i $|G| = |H|$, tada je $G \cong H$.*

Zatim ćemo definirati grupu kvaterniona i diedralnu grupu te dokazati tvrdnje o njihovim prezentacijama. Za kraj, dokazat ćemo da je svaka neabelova grupa reda 6 nužno izmorfna grupi S_3.

Poglavlje 1

Uvodne definicije i pojmovi

Kako bismo proučili pojam slobodne grupe, prvo je potrebno definirati što je grupa, a što njezina podgrupa te kada kažemo da je neka podgrupa normalna. Uz to, za razumijevanje rada bit će nam potrebno poznavanje pojmova kvocijentni skup i kvocijentna grupa te određenih preslikavanja među grupama poput homomorfizma i izomorfizma tako da ih u ovom poglavlju sve navodimo.

1.1 Definicije

Definicija 1.1. *Neka je G neprazan skup. Binarna operacija na skupu G je svako preslikavanje $\cdot : G \times G \to G$.*
Ako je $\cdot$ binarna operacija na G, uređeni par $(G, \cdot)$ nazivamo ***grupoid****.*

Definicija 1.2. *Neka je $(G, \cdot)$ grupoid. Kažemo da je $(G, \cdot)$* ***grupa*** *ako vrijede sljedeća svojstva:*

1. ***Svojstvo asocijativnosti:***

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

Grupoid sa ovim svojstvom nazivamo ***polugrupa****.*

2. ***Postojanje neutralnog elementa:***

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

Polugrupu sa ovim svojstvom nazivamo ***monoid****.*

3. ***Postojanje inverznog elementa:***

$$(\forall a \in G) \quad (\exists a' \in G) \quad a \cdot a' = a' \cdot a = e$$

Monoid sa ovim svojstvom nazivamo ***grupa****.*

Posebno, ako uz to vrijedi:

4. ***Svojstvo komutativnosti:***

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

za grupu $(G, \cdot)$ *kažemo da je* ***komutativna*** *ili* ***Abelova grupa****.*

Definicija 1.3. *Podskup* $H \subseteq G$ *je* ***podgrupa*** *od* G *ako je* $(H, \cdot)$ *također grupa, odnosno ako vrijedi:*

(i) $(\forall x, y \in H) \quad x \cdot y \in H$

(ii) $(\forall x \in H) \quad x^{-1} \in H$

Zapisujemo na sljedeći način: $H \leqslant G$

Definicija 1.4. *Podgrupa $N \leqslant G$ je **normalna** ako vrijedi: $xNx^{-1} = N$, $\forall x \in G$.*
Zapisujemo: $N \trianglelefteq G$.

Definicija 1.5. *Neka je G grupa i H njezina podgrupa. Definiramo relaciju ekvivalencije na G na sljedeći način. Za $x, y \in G$ vrijedi:*

$$x \sim y \Leftrightarrow xH = yH \Leftrightarrow x^{-1}y \in H$$

***Kvocijentni skup po relaciji** $\sim$ je skup svih klasa ekvivalencije, odnosno:*

$$G/_{\sim} = \{xH \mid x \in G\}$$

Kvocijentni skup od G po H zapisujemo: G/H

Teorem 1.6. *Neka je G grupa i $N \trianglelefteq G$. Tada je kvocijentni skup G/N uz operaciju:*

$$G/N \times G/N \to G/N$$

koja $(xN, yN) \mapsto xyN$ grupa.

Dokaz ovog teorema nalazi se u [1] na 49. stranici.

Definicija 1.7. *Grupu G/N iz Teorema 1.6 nazivamo **kvocijentna grupa od G po N**.*

1.2 Preslikavanja među grupama

Definicija 1.8. *Neka su G i H grupe. Preslikavanje $f : G \to H$ nazivamo **homomorfizam** ako:*

$$f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in G$$

Za homomorfizam $f : G \to H$ definiramo **jezgru:** $\operatorname{Ker} f = \{x \in G : f(x) = e_H\}$ i **sliku:** $\operatorname{Im} f = \{f(x) : x \in G\} \subseteq H$.

Napomena 1.9. *Posebno, ukoliko je funkcija f iz Definicije 1.8 injekcija, tada to preslikavanje nazivamo **monomorfizam**. Ukoliko je f surjekcija, nazivamo ga **epimorfizam** a ako je f bijekcija nazivamo ga **izomorfizam**.*

Definicija 1.10. *Dvije grupe G i H su **izomorfne** ako postoji izomorfizam $f : G \to H$. Zapisujemo: $G \cong H$*

Teorem 1.11. ***(Prvi teorem o izomorfizmu grupa)***
Neka je $f : G \to H$ homomorfizam. Tada je:

$$\operatorname{Ker} f \trianglelefteq G \quad i \quad G/\operatorname{Ker} f \cong \operatorname{Im} f.$$

Preciznije, ako je $\operatorname{Ker} f = K$, tada je preslikavanje $\varphi : G/K \to \operatorname{Im} f \subseteq H$, zadano pridružavanjem $\varphi : aK \mapsto f(a)$ izomorfizam.

Dokaz ovog teorema nalazi se u [1] na 50. i 51. stranici.

Teorem 1.12. ***(Treći teorem o izomorfizmu grupa)***
Neka je G grupa te neka su H i K normalne podgrupe grupe G takve da je $K \subseteq H$. Tada je $H/K \trianglelefteq G/K$ i vrijedi:

$$(G/K)/(H/K) \cong G/H.$$

Dokaz ovog teorema nalazi se u [1] na 52. i 53. stranici.

Poglavlje 2

Kategorije

Prije uvođenja pojma slobodne grupe, potrebno nam je poznavanje teorije kategorije. Uz njezinu definiciju, u ovom poglavlju navest ćemo i četiri primjera kategorija. Među njima, bit će spomenuta i kategorija grupa $\mathcal{G}$ koju ćemo proučavati u ovom radu. Definirat ćemo konkretnu kategoriju $\mathcal{C}$ i slobodni objekt F u njoj. Zatim ćemo taj isti objekt F promatrati u kategoriji grupa $\mathcal{G}$ što nas dovodi do definicije slobodne grupe. Pokazat ćemo i kada su dva slobodna objekta F i F' ekvivalentna te definirati inicijalni objekt u kategoriji $\mathcal{C}$.

Definicija 2.1. ***Kategorija*** $\mathcal{C}$ *je klasa objekata koje označavamo sa* $(A, B, C, \ldots)$ *zajedno sa:*

(i) *klasom disjunktnih skupova za svaki par objekata iz* $\mathcal{C}$ *koju označavamo sa* $hom(A, B)$. *Elemente* $f \in hom(A, B)$ *nazivamo* ***morfizmi*** *iz* A *u* B *i označavamo sa* $f : A \to B$.

(ii) *funkcijom za svaku trojku* (A, B, C) *objekata od* $\mathcal{C}$ *:*

$$hom(B, C) \times hom(A, B) \to hom(A, C)$$

Za morfizme $f : A \to B$ *i* $g : B \to C$ *ovu funkciju možemo zapisati na sljedeći način:* $(g, f) \longmapsto g \circ f$ *i pritom* $g \circ f : A \to C$ *nazivamo* ***kompozicija*** *od* f *i* g.

Pritom moraju biti zadovoljeni sljedeći aksiomi:

1. ***Aksiom asocijativnosti.***

   Ako su $f : A \to B$, $g : B \to C$ *i* $h : C \to D$ *morfizmi od* $\mathcal{C}$*, tada vrijedi:*

   $$h \circ (g \circ f) = (h \circ g) \circ f$$

2. ***Aksiom identitete.***

   Za svaki objekt B *od* $\mathcal{C}$ *postoji morfizam* $1_B : B \to B$ *takav da za svaki* $f : A \to B$ *i* $g : B \to C$ *vrijedi:*

   $$1_B \circ f = f \quad i \quad g \circ 1_B = g$$

Sukladno definiciji, navedimo nekoliko primjera kategorija.

Primjer 2.2.

(i) ***Kategorija skupova*** $\mathcal{S}$

Objekti u kategoriji $\mathcal{S}$ *su skupovi, morfizmi su funkcije a kompozicija je uobičajena kompozicija funkcija.*

Standardni rezultat teorije skupova kaže da je $hom(A, B)$*, klasa svih funkcija sa skupa* A *u skup* B*, skup. Činjenica da su morfizmi u parovima disjunktni skupovi proizlazi iz definicije jednakosti funkcija koja kaže da su dvije funkcije jednake ukoliko im se domena i kodomena podudaraju.*

(ii) ***Kategorija grupa*** $\mathcal{G}$

Objekti u kategoriji $\mathcal{G}$ *su grupe, morfizmi su homomorfizmi a kompozicija je uobičajena kompozicija homomorfizama.*

(iii) ***Kategorija Abelovih grupa*** $\mathcal{A}$

Objekti u kategoriji $\mathcal{A}$ *su Abelove grupe, morfizmi su homomorfizmi Abelovih grupa a kompozicija je uobičajena kompozicija homomorfizama.*

(iv) ***Kategorija komutativnih prstena*** $\mathcal{R}$

Objekti u kategoriji $\mathcal{R}$ *su komutativni prsteni, morfizmi su homomorfizmi prstenova a kompozicija je uobičajena kompozicija prstenova.*

Još neki primjeri kategorija mogu se pronaći u [2] na 53. stranici.

U ovom radu usredotočit ćemo se uglavnom na proučavanje slučaja **(ii)** iz Primjera 2.2, odnosno promatrat ćemo kategoriju grupa $\mathcal{G}$. U toj kategoriji svaki njezin objekt je skup (obično sa nekom dodatnom strukturom), a svaki morfizam $f : A \to B$ je funkcija na nekom pripadnom skupu (također sa nekim dodatnim svojstvom).

Tu ideju formalno zapisujemo pomoću sljedeće definicije:

Definicija 2.3. *Neka je objekt* $A \in \mathcal{C}$. ***Konkretna kategorija*** *je kategorija* $\mathcal{C}$ *zajedno sa funkcijom* σ *koja svakom* A *pridružuje skup* $\sigma(A)$. *Pritom* $\sigma(A)$ *nazivamo* ***pripadni skup*** *od* A.
On ima sljedeća svojstva:

1. *Svaki morfizam* $A \to B$ *iz* $\mathcal{C}$ *je funkcija na pripadnim skupovima* $\sigma(A) \to \sigma(B)$.
2. *Morfizam* $1_A : A \to A$ *je funkcija identite* $I_{\sigma(A)} : \sigma(A) \to \sigma(A)$.
3. *Kompozicija morfizama je kompozicija funkcija na pripadajućim skupovima.*

Prema tome, zaključujemo da je kategorija grupa $\mathcal{G}$ zajedno s funkcijom koja svakoj grupi pridružuju njezin pripadni skup (u uobičajenom smislu) konkretna kategorija.

Sada ćemo u proizvoljnoj konkretnoj kategoriji $\mathcal{C}$ definirati slobodni objekt nad nekim nepraznim skupom a nakon toga ćemo taj objekt promatrati i u kategoriji grupa $\mathcal{G}$.

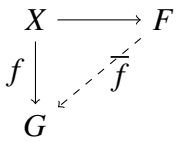
Definicija 2.4. *Neka je F objekt u konkretnoj kategoriji $\mathcal{C}$, X neprazan skup i $i : X \to F$ preslikavanje između skupova. Kažemo da je F* ***slobodan nad skupom*** *X ako za svaki objekt $A \in \mathcal{C}$ i za svaki $f : X \to A$ postoji jedinstveni morfizam $\overline{f} : F \to A$ takav da vrijedi:*

$$\overline{f} \circ i = f$$

Promotrimo li objekt F u kategoriji grupa $\mathcal{G}$ dolazimo do sljedeće definicije.

Definicija 2.5. *Neka je X podskup grupe F. Kažemo da je F* ***slobodna grupa s bazom*** *X ako za svaku grupu G i svaku funkciju $f : X \to G$ postoji jedinstveni homomorfizam $\overline{f} : F \to G$ takav da vrijedi: $\overline{f}(x) = f(x)$, $\forall x \in X$.*

Tvrdnju Definicije 2.5 možemo prikazati i sljedećim dijagramom:



Drugim riječima, zaključujemo da je slobodna grupa F slobodni objekt u kategoriji grupa $\mathcal{G}$. Međutim, s obzirom da ne znamo postoji li takav objekt u kategoriji grupa $\mathcal{G}$, u idućem poglavlju bavit ćemo se upravo konstrukcijom slobodne grupe.

Pokažimo sada kada su dva slobodna objekta ekvivalentna.

Teorem 2.6. *Neka je $\mathcal{C}$ konkretna kategorija, F i F' su objekti iz $\mathcal{C}$ takvi da je F slobodni nad skupom X i F' slobodni nad skupom X' te neka je $|X| = |X'|$. Tada vrijedi: $F = F'$.*

Dokaz. S obzirom da su F i F' slobodni objekti i $|X| = |X'|$, postoji bijekcija $f : X \to X'$ te preslikavanja $i : X \to F$ i $j : X' \to F'$.

Promotrimo preslikavanje $jf : X \to F'$. S obzirom da je F slobodni objekt, postoji morfizam $\varphi : F \to F'$ takav da sljedeći dijagram komutira:

$$\begin{array}{ccc} F & \xrightarrow{\varphi} & F' \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle j} \\ X & \xrightarrow[f]{} & X' \end{array}$$

Slično, s obzirom da bijekcija f ima inverz $f^{-1} : X' \to X$ i F' je slobodni objekt, postoji morfizam $\psi : F' \to F$ takav da sljedeći dijagram komutira:

$$\begin{array}{ccc} F' & \xrightarrow{\psi} & F \\ {\scriptstyle j}\uparrow & & \uparrow{\scriptstyle i} \\ X' & \xrightarrow[f^{-1}]{} & X \end{array}$$

Kombiniranjem ovih dijagrama dobivamo sljedeći komutativni dijagram:

$$\begin{array}{ccc} F & \xrightarrow{\psi \circ \varphi} & F \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i} \\ X & \xrightarrow[f^{-1}f = 1_X]{} & X \end{array}$$

Stoga vrijedi: $(\psi \circ \varphi)i = i1_X = i$. Međutim, vrijedi također: $1_F i = i$. Zaključujemo da prema Definiciji 2.4 mora vrijedi: $\psi \circ \varphi = 1_F$. Slično, vrijedi: $\varphi \circ \psi = 1_{F'}$.
Dakle, slobodni objekt F ekvivalentan je slobodnom objektu F'.

□

Na kraju ovog poglavlja, navedimo još i definiciju inicijalnog objekta u kategoriji $\mathcal{C}$.

Definicija 2.7. *Za objekt $I \in \mathcal{C}$ kažemo da je **inicijalni objekt** ako za svaki objekt $C \in \mathcal{C}$ postoji jedinstveni morfizam $f : I \to C$.*

Poglavlje 3

Konstrukcija slobodne grupe F

U ovom poglavlju definirat ćemo pojmove riječ, inverz neprazne riječi, podriječ te reducirana riječ. Zatim ćemo definirati operacije izravnog dopisivanja i elementarnog skraćivanja te pokazati da je njihova kombinacija dobro definirana operacija. Konačno, pokazat ćemo da skup svih reduciranih riječi na skupu X sa tom operacijom odgovara pojmu slobodne grupe sa bazom X. Na kraju ćemo još pokazati kada su dvije slobodne grupe izomorfne.

Definicija 3.1. *Neka je X skup koji nazivamo **abeceda**. Ako je n pozitivan broj, **riječ w** nad X duljine $n \geq 1$ je funkcija $w : \{1, 2, \ldots, n\} \to X$. Duljinu riječi w označimo sa $|w| = n$. Neka je 1 simbol koji nije sadržan u X. Njega nazivamo **praznom riječju** odnosno riječ duljine 0.*

Prema tome, riječ w nad X duljine $n \geq 1$ je n-torka koja leži nad X^n. S obzirom da $1 \notin X$, prazna riječ ne pojavljuje se u zapisu neprazne riječi. Nepraznu riječ označavamo na sljedeći način:
Ako je $w(i) = a_i \in X$ tada

$$w = a_1 \cdots a_n$$

S obzirom da je iz Definicije 3.1 vidljivo da je neprazna riječ funkcija, na neprazne riječi možemo primijeniti definiciju jednakosti funkcija i to na sljedeći način.

Ako su $u = a_1 \cdots a_n$ i $v = a'_1 \cdots a'_m$ neprazne riječi nad X tada je $u = v$ ako i samo ako je $n = m$ i $a_i = a'_i$, $\forall i$. Zaključujemo da svaka riječ nad X ima jedinstveni zapis.

Prisjetimo se sada kako smo definirali polugrupu i monoid. Prema Definiciji 1.2, polugrupa je grupoid sa svojstvom asocijativnosti, a monoid je polugrupa sa neutralnim elementom. Obje ove strukture prije svega su grupoidi, odnosno uređeni par skupa i binarne operacije nad tim skupom. Definirajmo sada binarnu operaciju nad skupom svih riječi nad abecedom X.

Definicija 3.2. *Ako je X skup, sa X^* označimo skup svih riječi nad abecedom X, uključujući i praznu riječ 1 (ukoliko je $X = \emptyset$, tada se X^* sastoji samo od prazne riječi). Nad skupom X^* definiramo binarnu operaciju koju nazivamo* ***izravno dopisivanje****.*
Za svaku riječ u definiramo $1u = u = u1$. Ako su $u = a_1 \cdots a_n$ i $v = a'_1 \cdots a'_m$ neprazne riječi nad X, definiramo:

$$uv = a_1 \cdots a_n a'_1 \cdots a'_m$$

Uočimo da vrijedi: $|uv| = |u| + |v|$ te da je izravno dopisivanje asocijativna operacija. Odnosno, ako je $w = a''_1 \cdots a''_k$ tada su $(uv)w$ i $u(vw)$ obje $(n + m + k)$-orke čije su j-koordinate jednake za svaki j. Prema tome, slijedi da je X^* nekomutativni monoid čiji je neutralni element neprazna riječ.

Neka je dan skup X te neka je X^{-1} njemu disjunktan skup takav da postoji bijekcija $X \to X'$ zadana pridruživanjem $x \mapsto x^{-1}$. Pretpostavimo da prazna riječ nije sadržana ni u jednom

od ovih skupova. Definiramo novu abecedu:

$$X \cup X^{-1}$$

Neprazna riječ $w \in (X \cup X^{-1})^*$ ima jedinstveni zapis:

$$w = x_1^{e_1} \cdots x_n^{e_n}$$

pri čemu je $x_i \in X$ i $e_i = \pm 1$ ($x \in X$ označimo sa x^1). S obzirom da $1 \notin X \cup X^{-1}$, prazna riječ 1 ne pojavljuje u zapisu neprazne riječi. Pišemo:

$$X^{**} = (X \cup X^{-1})^*$$

Inverz neprazne riječi definiramo na sljedeći način:

Definicija 3.3. ***Inverz*** *neprazne riječi* $w = x_1^{e_1} \cdots x_n^{e_n}$ *je:*

$$w^{-1} = (x_1^{e_1} \cdots x_n^{e_n})^{-1} = x_n^{-e_n} \cdots x_1^{-e_1}$$

Prazna riječ je sama sebi inverz.

Prema tome, slijedi da je $(w^{-1})^{-1} = w$ za svaki riječ w. Uočimo da je umnožak xx^{-1} u X^{**} riječ duljine 2, odnosno nije prazna riječ. Prema tome, monoid X^{**} je naša prva aproksimacija prema konstrukciji slobodne grupe sa bazom X. Činjenica da je $xx^{-1} \neq 1$ pokazuje nam da X^{**} nije grupa.

Definicija 3.4. ***Podriječ*** *neprazne riječi* $w = x_n^{e_n} \cdots x_1^{e_1} \in X^{**}$ *je ili prazna riječ ili riječ oblika:*

$$u = x_r^{e_r} \cdots x_s^{e_s}$$

gdje je $1 \leqslant r \leqslant s \leqslant n$.

Ako je:

- $x_r^{e_r} \cdots x_s^{e_s}$ podriječ od w, tada možemo pisati: $w = Ax_r^{e_r} \cdots x_s^{e_s} B$, gdje su A i B podriječi od w
- $r = 1$ tada $A = 1$ i $x_r^{e_r} \cdots x_s^{e_s}$ je inicijalni segment od w
- $s = n$ tada $B = 1$ i $x_r^{e_r} \cdots x_s^{e_s}$ je terminalni segment od w

Najvažnije riječi su reducirane riječi.

Definicija 3.5. *Riječ $w \in X^{**}$ je **reducirana** ako je $w = 1$ ili ako w nema podriječi oblika xx^{-1} ili $x^{-1}x$ za neki $x \in X$.*

Uočimo da je svaka podriječ reducirane riječi reducirana.

Ukoliko riječ w nije reducirana, potrebno je uvesti novu operaciju.

Definicija 3.6. *Ako $w \in X^{**}$ nije reducirana, tada ona sadrži podriječ oblika $x^e x^{-e}$, gdje je $x \in X$ i $e = \pm 1$. Zapisujemo:*

$$w = Ax^e x^{-e} B$$

*Ako je $w_1 = AB$ tada kažemo da je $w \to w_1$ **elementarno skraćivanje**.*
*Ako riječ w nije reducirana tada je **redukcija** od w konačan slijed skraćivanja:*

$$w \to w_1 \to \cdots \to w_r$$

pri čemu je w_r reducirana riječ.

Ako je w bilo koja riječ, tada postoji redukcija $ww^{-1} \to w_1 \to \cdots \to 1$.

Lema 3.7. *Ako je $w \in X^{**}$, tada je w ili reducirana riječ ili postoji redukcija:*

$$w \to w_1 \to \cdots \to w_r.$$

Dokaz. Dokazujemo indukcijom za $|w| \geq 0$. Kad je $|w| = 0$ ili $|w| = 1$, tada tvrdnja po definiciji vrijedi. Pretpostavimo da tvrdnja vrijedi za w, $|w| < n$, $n \in \mathbb{N}$. Pokažimo da tvrdnja vrijedi kad je $|w| = n$.

Ukoliko w nije reducirana riječ i $w \to w_1$ je elementarno skraćivanje, tada vrijedi:

$$|w_1| = |w| - 2$$

odnosno $|w_1| < n$ pa možemo primijeniti pretpostavku indukcije.
Prema pretpostavci indukcije, ili je w_1 reducirana ili postoji redukcija $w_1 \to \cdots \to w_r$ pa je stoga $w \to w_1 \to \cdots \to w_r$ redukcija od w. □

Prirodno je pokušati definirati slobodnu grupu sa bazom X kao skup $\mathcal{R}$ koji čine sve reducirane riječi u X^{**} sa operacijom izravnog dopisivanja kao binarnom operacijom. No međutim, to nije dovoljno dobro s obzirom da skup $\mathcal{R}$ nije zatvoren, odnosno činjenica da su u i v reducirane riječi ne povlači da je uv također reducirana. Stoga je potrebno operaciju izravnog dopisivanja kombinirati zajedno sa operacijom elementarnog skraćivanja. Lema 3.8 pokazuje nam da je ta nova binarna operacija dobro definirana.

Lema 3.8. *Neka je X skup i $w \in X^{**}$. Ako su:*

$$w \to w_1 \to w_2 \to \cdots \to w_r \quad i \quad w \to w_1{}' \to w_2{}' \to \cdots \to w_q{}'$$

redukcije, tada je $w_r = w_q{}'$.

Dokaz. Dokazujemo indukcijom za $|w| \geq 0$. Kad je $|w| = 0$ ili $|w| = 1$, tada tvrdnja po definiciji vrijedi. Pretpostavimo da tvrdnja vrijedi za w, $|w| < n$, $n \in \mathbb{N}$. Pokažimo da tvrdnja vrijedi kad je $|w| = n$.

Tvrdimo da je $w_1 = w_1{}'$ ili postoji $z \in X^{**}$ i elementarno skraćivanje $w_1 \to z$ i $w_1{}' \to z$.

Razlikujemo dva slučaja:

1° Pretpostavimo:

$$w = Ass^{-1}Btt^{-1}C$$

gdje su $s, t \in X \cup X^{-1}$, $w_1 = ABtt^{-1}C$ i $w_1{}'' = Ass^{-1}BC$.
U tom slučaju: $z = ABC$.

2° Neka je:

$$w = Ass^{-1}sB$$

tada elementarno skraćivanje $w \to w_1$ briše ss^{-1} a skraćivanje $w \to w_1{}'$ briše $s^{-1}s$.
U tom slučaju: $w_1 = AsB = w_1{}'$ i prema tome, tvrdnja je istinita.

Za korak indukcije odaberemo redukciju $z \to \cdots \to w_d{}''$.

Pretpostavku indukcije najprije primijenimo na redukcije:

$$w_1 \to w_2 \to \cdots \to w_r \quad \text{i} \quad w_1 \to z \to \cdots \to w_d{}''$$

Kako je $|w_1| < |w|$ možemo primijeniti pretpostavku indukcije:

$$w_r = w_d{}''$$

Slično, pretpostavku primijenimo i na redukcije:

$$w_1{}' \to z \to \cdots \to w_q{}' \quad \text{i} \quad w_1{}' \to w_2{}' \to \cdots \to w_d{}''$$

Iz $|w_1{}'| < |w|$ slijedi:

$$w_d{}'' = w_q{}'$$

Iz gornje dvije jednakosti slijedi:

$$w_r = w_q{}'$$

što smo i htjeli dokazati.

□

Iz Leme 3.8 slijedi da sve redukcije neke riječi $w \in X^{**}$ završavaju sa istom reduciranom riječju, označimo je sa w_r. Reduciranu riječ sada možemo zapisati na sljedeći način:

$$red(w) = w_r.$$

Na ovaj način dobivamo tvrdnju Korolara 3.9.

Korolar 3.9. *Ako je $F(X)$ skup svih reduciranih riječi na X tada je:*

$$u * v = red(uv)$$

dobro definirana operacija na $F(X)$.

Ako su u i v reducirane riječi za koje vrijedi da je umnožak uv također reduciran, tada vrijedi:

$$u * v = uv$$

Posebno, ako je $u = {x_1}^{e_1} \cdots {x_n}^{e_n}$ reducirana riječ tada je:

$$u = {x_1}^{e_1} * u'$$

gdje je $u' = x_2^{e_2} \cdots {x_n}^{e_n}$.

Nakon što smo pokazali da je $u * v$ dobro definirana operacija, možemo iskazati i dokazati sljedeći teorem.

Teorem 3.10. *Ako je X skup, $F(X)$ je skup svih reduciranih riječi na X. Skup $F(X)$ sa binarnom operacijom $u * v = red(uv)$ je **slobodna grupa** sa bazom X.*

Prije samog dokaza, uočimo da vrijedi sljedeće: prazna riječ 1 kao neutralni element i inverz neprazne riječi iz Definicije 3.3 zadovoljavaju aksiome grupe. Dakle, sve što je potrebno provjeriti da bi dokazali da je $F(X)$ grupa jest da vrijedi asocijativnost.

Dokaz. Neka su dane reducirane riječi u, v i y. Definiramo $w = uvy$ u X^{**}.

Iz Leme 3.8 slijedi da redukcije:

$$w = (uv)y \to \cdots \to (u * v)y \to \cdots \to w_r$$

i

$$w = u(vy) \to \cdots \to u(v * y) \to \cdots \to {w_q}'$$

imaju isti reducirani kraj:

$$w_r = {w_q}'$$

Stoga vrijedi:

$$(u * v) * y = u * (v * y)$$

Prema tome, $F(X)$ je grupa.

Dokažimo sada još da je $F(X)$ slobodna grupa.

Neka je G grupa i $f : X \to G$ funkcija. Ako je $u \in F(X)$, tada je u reducirana riječ i ima jedinstveni zapis:

$$u = {x_1}^{e_1} \cdots {x_n}^{e_n}$$

Definiramo funkciju:

$$\varphi : F(X) \to G$$

sa $\varphi(1) = 1$ i $\varphi(u) = \varphi(x_1^{e_1} \cdots {x_n}^{e_n}) = f(x_1)^{e_1} \cdots f(x_n)^{e_n}$.

Dovoljno je dokazati da je φ homomorfizam, jedinstvenost će slijedi iz toga da se $F(X)$ generira nad X.

Ako su $u, v \in F(X)$, dokažemo da je:

$$\varphi(u * v) = \varphi(u)\varphi(v)$$

pomoću indukcije za $|u| + |v| \geq 0$.

Za bazu $|u| + |v| = 0$, tvrdnja je istinita, odnosno: $\varphi(1 * 1) = \varphi(1) = 1 = \varphi(1)\varphi(1)$. Točnije, $\varphi(1 * v) = \varphi(1)\varphi(v)$ pa možemo pretpostaviti da početni korak dokazujemo za $|u| \geq 1$.

Zapišemo reduciranu riječ $u = x^e u'$, gdje je $u' = {x_2}^{e_2} \cdots {x_n}^{e_n}$ i s obzirom da je ta riječ reducirana vrijedi:

$$\varphi(u) = f(x)^e f(x_2)^{e_2} \cdots f(x_n)^{e_n} = \varphi(x^e)\varphi(u')$$

Sada je $u * v = x^e * (u' * v)$ pa reduciranu riječ možemo zapisati na sljedeći način:

$$u' * v = {z_1}^{c_1} \cdots {z_t}^{c_t}$$

gdje je $z_1, \cdots z_t \in X$.

Razlikujemo sva slučaja:

1° Ako je $x^e \neq {z_1}^{-c_1}$, tada je $x^e {z_1}^{c_1} \cdots {z_t}^{c_t}$ reducirana i iz definicije funkcije φ slijedi:

$$\begin{aligned}\varphi(u * v) &= \varphi(x^e * u' * v) = \varphi(x^e {z_1}^{c_1} \cdots {z_t}^{c_t}) \\ &= f(x)^e f(z_1)^{c_1} \cdots f(z_t)^{c_t} \\ &= \varphi(x^e)\varphi(u' * v) \\ &= \varphi(x^e)\varphi(u')\varphi(v) \\ &= \varphi(u)\varphi(v)\end{aligned}$$

2° Ako je $x^e = {z_1}^{-c_1}$ tada je:

$$u * v = x^e * u' * v = {z_2}^{c_2} \cdots {z_t}^{c_t}$$

Stoga vrijedi:

$$\begin{aligned}\varphi(u * v) &= \varphi(x^e * u' * v) \\ &= \varphi({z_2}^{c_2} \cdots {z_t}^{c_t}) \\ &= f(z_2)^{c_2} \cdots f(z_t)^{c_t} \\ &= [f(x)^e f(z_1)^{c_1}] f(z_2)^{c_2} \cdots f(z_t)^{c_t} \\ &= \varphi(x^e)\varphi(u' * v) \\ &= \varphi(x^e)\varphi(u')\varphi(v) \\ &= \varphi(u)\varphi(v)\end{aligned}$$

Zbog toga jer je:

$$f(x)^e f(z_1)^{c_1} = 1$$

φ je homomorfizam, a $F(X)$ je slobodna grupa sa bazom X čime je dokaz gotov.

□

Od sada nadalje, množenje $u * v = red(uv)$ zapisivat ćemo samo kao uv.

Pokažimo još kada su dvije slobodne grupe izomorfne.

Propozicija 3.11.

(i) *Neka je X_1 baza slobodne grupe F_1 te neka je X_2 baza slobodne grupe F_2. Ukoliko postoji bijekcija $f : X_1 \to X_2$ tada je: $F_1 \cong F_2$.*
Drugim riječima, postoji izomorfizam $\varphi_1 : F_1 \to F_2$ koji je proširenje od f.

(ii) *Ako je $F(X)$ slobodna grupa sa bazom X, tada je $F(X)$ generirana sa X.*

Dokaz.

(i) S obzirom da smo u Teoremu 2.6 pokazali da tvrdnju sličnu ovoj možemo primijeniti na slobodne objekte F nad skupom X i F' nad skupom X', a u Teoremu 3.10 pokazali smo da je svaki slobodni objekt $F(X)$ slobodna grupa sa bazom X zaključujemo da se dokaz ove tvrdnje provodi analogno dokazu Teorema 2.6.

(ii) Ako je $F(X)$ slobodna grupa sa bazom X konstruirana kao u Teoremu 3.10 tada X generira $F(X)$. Iz Propozicije 3.11 (i) zaključujemo da postoji izomorfizam $\varphi : F(X) \to F$ definiran sa $\varphi(X) = X$ (ukoliko je $f : X \to X$ identiteta 1_X). S obzirom da X generira $F(X)$, $\varphi(X) = X$ generira $\operatorname{Im}\varphi = F$ što zapravo znači da X generira F.

□

Poglavlje 4

Slobodne Abelove grupe

U ovom poglavlju navest ćemo najvažnije rezultate vezane za slobodne Abelove grupe koje ćemo kasnije primijeniti na slobodne grupe. Slobodnu Abelovu grupu definiramo kao sumu beskonačnih cikličkih grupa i pokazujemo da je slobodna Abelova grupa slobodni objekt nad nekim skupom u kategoriji Abelovih grupa. Nadalje, definiramo rang slobodne Abelove grupe i pokazujemo da rang ne ovisi o izboru baze. Također, pokazat ćemo da su dvije slobodne Abelove grupe izomorfne ako i samo ako su istog ranga. Na kraju poglavlja, definirat ćemo komutator i komutatorsku podgrupu te navesti propoziciju koja generalizira činjenicu kada dva elementa x i y neke grupe G komutiraju.

Za definiranje slobodne Abelove grupe, najprije je potrebno poznavanje sljedeće definicije:

Definicija 4.1. *Ako su $S_1, \ldots, S_n$ podgrupe Abelove grupe F, njihovu (unutarnju)* ***direktnu sumu*** *definiramo indukcijom za $n \geq 2$:*

$$S_1 \oplus \cdots \oplus S_{n+1} = (S_1 \oplus \cdots \oplus S_n) \oplus S_{n+1}$$

Direktnu sumu $S_1 \oplus \cdots \oplus S_n$ možemo označiti i kao $\bigoplus_{i=1}^{n} S_i$.

Definicija 4.2. *Ako su* $\langle x_1\rangle, \ldots, \langle x_n\rangle$ *beskonačne cikličke grupe, tada njihovu direktnu sumu:*

$$F = \langle x_1\rangle \oplus \cdots \oplus \langle x_n\rangle$$

nazivamo ***slobodna Abelova grupa*** *sa bazom* $X = \{x_1, \ldots, x_n\}$. *Općenito, svaku grupu izomorfnu F nazivamo slobodna Abelova grupa.*

Primjerice, $\mathbb{Z}^m = \mathbb{Z} \times \cdots \times \mathbb{Z}$ grupa svih m-torki $(n_1, \ldots, n_m)$ cijelih brojeva jest slobodna Abelova grupa. Jedna baza od $\mathbb{Z}^m$ je standardna baza $e_1, \ldots, e_m$ gdje je e_i m-torka koja ima jedinicu na i-tom mjestu a nulu na ostalima.

Prirodno je slobodnu Abelovu grupu definirati kao slobodni objekt u kategoriji slobodnih Abelovih grupa što ćemo kasnije pokazati pomoću Teorema 4.7 no za potrebe ovog poglavlja odlučili smo se za Definiciju 4.2.

Tvrdnju sljedeće propozicije iskazat ćemo za Abelove grupe ali njezin dokaz možemo primijeniti i na neabelove grupe ako pretpostavimo da su H_i normalne podgrupe.

Propozicija 4.3. *Ako su* $G_1, \ldots, G_2$ *(Abelove) grupe i* $H_i \subseteq G_i$ *podgrupe, tada vrijedi:*

$$(G_1 \times \cdots \times G_n)/(H_1 \times \cdots \times H_n) \cong (G_1/H_1) \times \cdots \times (G_n/H_n).$$

Dokaz. Funkcija $f : G_1 \times \cdots \times G_n \to (G_1/H_1) \times \cdots \times (G_n/H_n)$ zadana pridruživanjem $f : (g_1, \ldots, g_n) \mapsto (g_1 + H_1, \ldots, g_n + H_n)$ je surjektivni homomorfizam za koji vrijedi da je: $\operatorname{Ker} f = H_1 \times \cdots \times H_n$. S obzirom da je $\operatorname{Im} f \leqslant (G_1/H_1) \times \cdots \times (G_n/H_n)$, tvrdnja slijedi iz Teorema 1.11. □

Propozicija 4.4. $\mathbb{Z}^m \cong \mathbb{Z}^n$ *ako i samo ako je* $m = n$.

Dokaz. Uočimo najprije da vrijedi sljedeće: ako je Abelova grupa G jednaka direktnoj sumi $G = G_1 \oplus \cdots \oplus G_n$, tada je $2G = 2G_1 \oplus \cdots \oplus 2G_n$. Iz Propozicije 4.3 slijedi da je:

$$G/2G \cong (G_1/2G_1) \oplus \cdots \oplus (G_n/2G_n).$$

Općenito, ako je $G = \mathbb{Z}^n$, tada je $|G/2G| = 2^n$. Konačno, ako je $\mathbb{Z}^n \cong \mathbb{Z}^m$, tada je $\mathbb{Z}^n/2\mathbb{Z}^n \cong \mathbb{Z}^m/2\mathbb{Z}^m$ i $2^n = 2^m$. Zaključujemo da vrijedi: $n = m$. □

Posljedica Propozicije 4.4 jest tvrdnja sljedećeg Korolara.

Korolar 4.5. *Ako je F slobodna Abelova grupa, tada bilo koje dvije (konačne) baze od F imaju jednak broj elemenata.*

Dokaz. Ako je $\{x_1, \ldots, x_n\}$ baza od F, tada je $F \cong \mathbb{Z}^n$. Ako je $\{y_1, \ldots, y_m\}$ neka druga baza od F tada je $F \cong \mathbb{Z}^m$. Prema Propoziciji 4.4, $m = n$. □

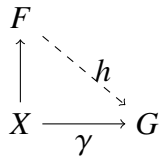
Definicija 4.6. *Ako je F slobodna Abelova grupa sa bazom $\{x_1, \ldots, x_n\}$, tada n nazivamo **rang** od F i zapisujemo: $rang(F) = n$.*

Korolar 4.5 kaže nam je $rang(F)$ dobro definiran, odnosno da ne ovisi o izboru baze. U tom smislu, Propozicija 4.4 kaže da su dvije slobodne Abelove grupe izomorfne ako i samo su istog ranga.

Poput slobodnih grupa iz Definicije 2.5, slobodne Abelove grupe također možemo opisati pomoću univerzalnog svojstva. Kao što je već ranije spomenuto, tada je slobodna Abelova grupa slobodni objekt u kategoriji Abelovih grupa $\mathcal{A}$ iz Primjera 2.2 (iii).

Teorem 4.7. *Neka je F slobodna Abelova grupa sa bazom $X = \{x_1, \ldots, x_n\}$. Za svaku Abelovu grupu G i za svaku funkciju $\gamma : X \to G$ postoji jedinstveni homomorfizam $h : F \to G$ takav da vrijedi: $h(x_i) = \gamma(x_i)$, $\forall x_i$.*

Tvrdnju teorema možemo prikazati i sljedećim dijagramom.



Dokaz. Svaki element $a \in F$ ima jedinstveni zapis u obliku $a = \sum_{i=1}^{n} m_i x_i$, pri čemu je $m_i \in \mathbb{Z}$. Ta jedinstvenost povlači da je $h : F \to G$, definirana sa:

$$h(a) = \sum_{i=1}^{n} m_i \gamma(x_i),$$

dobro definirana funkcija.

Neka je $b \in F$ neki drugi element slobodne Abelove grupe F koji ima jedinstveni zapis u obliku $b = \sum_{i=1}^{n} p_i x_i$. Tada vrijedi:

$$h(a \cdot b) = \sum_{i=1}^{n} m_i p_i (\gamma(x_i))^2 = \sum_{i=1}^{n} m_i \gamma(x_i) \cdot \sum_{i=1}^{n} p_i \gamma(x_i) = h(a) \cdot h(b)$$

odnosno, $h : F \to G$ je homomorfizam.

Ako je $h' : F \to G$ homomorfizam takav da vrijedi $h'(x_i) = h(x_i)$, $\forall i$ tada je $h' = h$. Odnosno, dva homomorfizma nad istim skupom generatora moraju biti jednaki čime je tvrdnja teorema dokazana. □

Propozicija 4.8. *Neka je $X = \{x_1, \ldots, x_n\}$ uređeni skup i A Abelova grupa. Neka za A vrijedi svojstvo iz Teorema 4.7: za svaku Abelovu grupu G i za svaku funkciju $\gamma : X \to G$ postoji jedinstveni homomorfizam $g : A \to G$ za koji vrijedi $g(x_i) = \gamma(x_i)$, $\forall x_i$. Tada je A slobodna Abelova grupa ranga n sa bazom X.*

Dokaz. Neka je $Y = e_1, \ldots, e_n$ baza od $\mathbb{Z}^n$ i neka su $k : Y \to \mathbb{Z}^n$ i $j : X \to A$ preslikavanja.

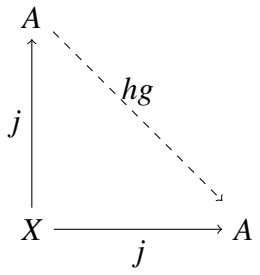
Proučimo sljedeći dijagram:

$$\begin{array}{ccc} & g & \\ A & \dashrightarrow & \mathbb{Z}^n \\ & \underset{h}{\dashleftarrow} & \\ {\scriptstyle j}\uparrow & & \uparrow{\scriptstyle k} \\ & q & \\ X & \rightleftarrows & Y \\ & p & \end{array} \tag{4.1}$$

Neka je $q(x_i) = e_i$ i $p(e_i) = x_i$, $\forall i$.

Prema svojstvu iz Teorema 4.7, postoji preslikavanje $g : A \to \mathbb{Z}^n$ definirano sa $gj = kq$ (za $kq : X \to \mathbb{Z}^n$). S obzirom da je $\mathbb{Z}^n$ slobodna Abelova grupa sa bazom Y, prema Teoremu 4.7 postoji i preslikavanje $h : \mathbb{Z}^n \to A$ definirano sa $hk = jp$.

Da bismo uočili da je $g : A \to \mathbb{Z}^n$ izomorfizam, proučimo sljedeći dijagram:



(4.2)

Kako bismo pokazali da dijagram (4.2) komutira, proučimo prethodno dobivene tvrdnje:

$$gj = kq$$

$$hk = jp$$

Pomnožimo li prvu sa h i drugu sa q dobivamo sljedeće:

$$gjh = kqh$$

$$hkq = jpq$$

Izjednačavanjem i korištenjem svojstva komutativnosti Abelove grupe, dobivamo sljedeću jednakost:

$$hgj = khq = jpq$$

No međutim, promotrimo li dijagram (4.1), uočavamo da vrijedi sljedeće:

$$khq = j$$

$$jpq = j$$

Drugim riječima, vrijedi:

$$hgj = khq = jpq = j$$

čime smo dokazali da dijagram (4.2) komutira.

Prema pretpostavci, hg je jedinstveni homomorfizam sa tim svojstvom. Međutim, 1_A je također takav homomorfizam pa je prema tome $hg = 1_A$. Sličan dijagram pokazuje nam da je $gh = 1_{\mathbb{Z}^n}$ pa su stoga g i h izomorfizmi.

Konačno, činjenica da je $\mathbb{Z}^n$ slobodna Abelova grupa s bazom Y povlači da je A slobodna Abelova grupa s bazom $X = h(Y)$.

□

Povezano sa pojmom slobodne Abelove grupe, navest ćemo definicije komutatora i komutatorske podgrupe koje će nam biti potrebne za razumijevanje sljedeće propozicije.

Definicija 4.9. *Ako je G grupa i $x, y \in G$ tada se njihov* ***komutator*** $[x, y]$ *definira kao:*

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

Ako su X i Y podgrupe grupe G, tada se $[X, Y]$ *definira kao:*

$$[X, Y] = \langle [x, y] : x \in X, y \in Y \rangle$$

Posebno, ***komutatorska podgrupa*** G' *grupe G je:*

$$G' = [G, G]$$

odnosno podgrupa generirana sa svim komutatorima.

Iz definicije je očito da dva elementa x i y grupe G komutiraju ako i samo ako je njihov komutator $[x, y] = 1$. Sljedeća propozicija generalizira tu činjenicu.

Propozicija 4.10. *Neka je G grupa.*

(i) *Komutatorska podgrupa G' je normalna podgrupa grupe G i G/G' je Abelova grupa.*

(ii) *Ako je $H \trianglelefteq G$ i G/H je Abelova grupa tada je $G' \subseteq H$.*

Dokaz.

(i) Inverz komutatora $xyx^{-1}y^{-1}$ je također komutator:

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

Stoga, svaki element od G' je umnožak komutatora. Ali svaki konjugator komutatora (samim time i umnožak komutatora) je komutator oblika:

$$\begin{aligned} a[x,y]a^{-1} &= a(xyx^{-1}y^{-1})a^{-1} \\ &= axa^{-1}aya^{-1}ax^{-1}a^{-1}ay^{-1}a^{-1} \\ &= [axa^{-1}, aya^{-1}] \end{aligned}$$

Stoga vrijedi: $G' \trianglelefteq G$.

Ako su $aG', bG' \in G/G'$ tada je:

$$aG'bG'(aG')^{-1}(bG')^{-1} = aba^{-1}b^{-1}G' = [a,b]G' = G'$$

pa je stoga G/G' Abelova grupa.

(ii) Pretpostavimo da je $H \trianglelefteq G$ i G/H Abelova grupa.
Ako su $a, b \in G$, tada vrijedi:

$$aHbH = bHaH \Rightarrow abH = baH \Rightarrow b^{-1}a^{-1}ba \in H$$

S obzirom da je svaki komutator oblika $b^{-1}a^{-1}ba$ slijedi da je $G' \subseteq H$.

□

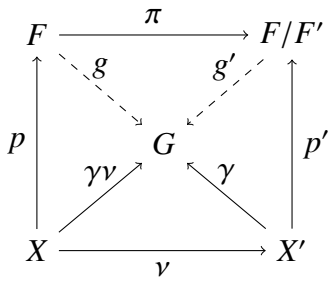
Poglavlje 5

Rang slobodne grupe

U ovom poglavlju pokazat ćemo vezu između tvrdnji navedenih u prethodna dva poglavlja. Konkretno, pokazat ćemo vezu slobodne grupe sa slobodnom Abelovom grupom i komutatorskom podgrupom. Nakon toga, dokazat ćemo propoziciju koja govori o broju elemenata baze slobodne grupe što će nas dovesti do definicije ranga slobodne grupe. Za kraj, pokazat ćemo kada su dvije slobodne grupe izomorfne.

Lema 5.1. *Neka je F slobodna grupa sa bazom X. Tada je F/F' slobodna Abelova grupa sa bazom $X' = \{xF' : x \in X\}$, gdje je F' komutatorska podgrupa grupe F.*

Dokaz. Uočimo najprije da iz Propozicije 3.11 (ii) slijedi da X' generira F/F'. Da je F/F' slobodna Abelova grupa sa bazom X' dokazat ćemo koristeći kriterij iz Propozicije 4.8. Promatramo sljedeći dijagram:



Ovdje je G proizvoljna Abelova grupa, p i p' preslikavanja takva da je $p : X \to F$ i $p' : X' \to F/F'$, a π je prirodno preslikavanje iz F u F/F', ν preslikavanje koje $\forall x \mapsto xF'$ i $\gamma : X' \to G$ proizvoljna funkcija.

Neka je $g : F \to G$ jedinstveni homomorfizam (iz Definicije 2.5) dan sa $gp = \gamma\nu$ (pritom je $\gamma\nu : X \to G$ funkcija). Definiramo preslikavanje $g' : F/F' \to G$ sa $wF' \mapsto g(w)$. Pritom je g' dobro definirana jer činjenica da je G Abelova grupa povlači da je $F' \subseteq Kerg$.

Zbog $g'p'\nu = g'\pi p = gp = \gamma\nu$ i jer je γ surjekcija, dobivamo:

$$g'p' = \gamma$$

Konačno, g' je jedinstveno takvo preslikavanje. Zaista, ako imamo g'' takvo da:

$$g''p' = \gamma$$

tada se g' i g'' podudaraju na generatorima skupa X' i prema tome moraju biti jednaki. □

Sljedeća propozicija govori o broju elemenata baze slobodne grupe.

Propozicija 5.2. *Neka je F slobodna grupa sa bazom X. Ukoliko je $|X| = n$ tada svaka baza od F ima n elemenata.*

Dokaz. Prema Lemi 5.1, F/F' je slobodna Abelova grupa ranga n. S druge strane, ukoliko je Y baza od F i $|Y| = m$ tada je F/F' slobodna Abelova grupa ranga m.
S obzirom da je F/F' slobodna Abelova grupa, iz Korolara 4.5 znamo da bilo koje dvije konačne baze od F/F' imaju jednak broj elemenata, iz čega slijedi da je: $m = n$. □

Sada možemo definirati rang slobodne grupe.

Definicija 5.3. ***Rang slobodne grupe*** *F je kardinalni broj od F. Označavamo ga sa: $rang(F)$.*

Slobodna grupa F konačnog ranga n obično se označava sa F_n. Ukoliko je njezina baza $X = \{x_1, \ldots, x_n\}$, možemo ju zapisati i kao $F_n(X)$ ili $F(x_1, \ldots, x_n)$.

Sada ćemo iskazati i dokazati teorem koji kaže kada su dvije slobodne grupe izomorfne.

Teorem 5.4. *Neka je F slobodna grupa s bazom X i G slobodna grupa sa bazom Y. Tada vrijedi:*

$$F \cong G \Leftrightarrow |X| = |Y|$$

Dokaz.

($\Rightarrow$) Ako je $\varphi : F \to G$ izomorfizam tada vrijedi: $F/F' \cong G/G'$.
Prema Lemi 5.1, F/F' je slobodna Abelova grupa sa bazom $X' = \{xF' : x \in X\}$. S obzirom da je $|X| = |X'|$ slijedi da je $|X| = rang(F/F')$. Analogno, $|Y| = rang(G/G')$ pa iz Propozicije 5.2 slijedi: $|X| = |Y|$.

($\Leftarrow$) Ovaj smjer već je dokazan za slobodne objekte u Teoremu 2.6, odnosno za slobodne grupe u Propoziciji 3.11 (i).

□

Teorem 5.4 nam zapravo kaže da rang slobodne grupe F ne ovisi o odabiru njezine baze.

Poglavlje 6

Prezentacije

U ovom poglavlju, osim što ćemo definirati prezentacije, dokazat ćemo i tvrdnju koja kaže da svaka grupa ima prezentaciju. Zatim ćemo proučiti par primjera prezentacija te reći nekoliko riječi o njihovom označavanju. Definirat ćemo tip grupe koji ćemo povezati s prezentacijama pomoću *von Dyck-ovog teorema*. Zatim ćemo proučiti dvije grupe, grupu kvaterniona i diedralnu grupu te dokazati tvrdnje o njihovim prezentacijama. Za kraj, dokazat ćemo da je svaka neabelova grupa reda 6 nužno izomorfna grupi S_3.

Propozicija 6.1. *Svaka grupa G je kvocijent slobodne grupe.*

Dokaz. Neka je X skup za koji postoji bijekcija $f : X \to G$. Na primjer, možemo smatrati da je X osnovni skup od G i $f = 1_G$. Neka je F slobodna grupa sa bazom X. Tada postoji homomorfizam $\varphi : F \to G$ koji je proširenje od f i s obzirom da je F surjektivan i φ je također. Stoga vrijedi:

$$G \cong F/\operatorname{Ker}\varphi.$$

□

Definicija 6.2. *Neka je X skup, $F = F(X)$ slobodna grupa s bazom X i $R \subseteq F$ skup riječi nad X. Grupa G ima* ***prezentaciju****:*

$$G = (X \mid R),$$

ako je $G \cong F/N$, pri čemu je N normalna podgrupa od F generirana sa R, odnosno N je najmanja normalna podgrupa od F koja sadrži R.

Pritom, skup X nazivamo **generatorima** a skup R **relacijama**. Izraz *generatori* se sada koristi u općenitom smislu, a za X koji nije podskup od G podskup $\{xN : x \in X\}$ generira F/N u uobičajenom smislu.

Propozicija 6.1 nam zapravo kaže da svaka grupa ima prezentaciju.

Prije nego što navedemo neke primjere prezentacija, definirajmo najprije grupe čije ćemo prezentacije promatrati.

Permutacija skupa X je bijekcija skupa X na samog sebe.

Definicija 6.3. *Familija svih permutacija skupa X, koju označavamo sa S_X, nazivamo* ***simetrična grupa nad*** *X. Kada je $X = \{1, 2, \ldots, n\}$, S_X označavamo sa S_n i nazivamo* ***simetrična grupa reda n****.*

Neka je $GL(n, \mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$ opća linearna grupa.

Definicija 6.4. *Definiramo $A, B \in GL(2, \mathbb{Q})$ sa $A = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ i $B = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]$.*
Kvocijentnu grupa $M = \langle A, B\rangle/N$, pri čemu je $N = \langle \pm I\rangle$ (I jedinična matrica) nazivamo ***modularna grupa****.*

Primjer 6.5.

(i) *Općenito, grupa može imati više različitih prezentacija. Na primjer, grupa* $G = \mathbb{I}_6$ *ima prezentacije:*

$$(x \mid x^6) \quad i \quad (a, b \mid a^3, b^2, aba^{-1}b^{-1}).$$

Uočimo što to znači: postoji izomorfizam $\mathbb{I}_6 \cong F(x)/\langle x^6 \rangle$ *i* $\mathbb{I}_6 \cong F(a, b)/N$*, pri čemu je* N *normalna podgrupa generirana sa* $a^3, b^2, aba^{-1}b^{-1}$*.*
Relacija $aba^{-1}b^{-1}$ *kaže da* a *i* b *komutiraju. Ukoliko zamijenimo taj komutator sa* $abab$*, tada imamo prezentaciju:* $(a, b \mid a^3, b^2, abab)$*. Riječ je o prezentaciji grupe* S_3*, simetrične grupe reda* 3 *iz Definicije 6.3.*
Obrišemo li tu relaciju, dobivamo prezentaciju: $(a, b \mid a^3, b^2)$*, a to je prezentacija beskonačne modularne grupe* M *iz Definicije 6.4.*

(ii) *Slobodna grupa s bazom* X *ima prezentaciju:*

$$(X \mid \emptyset).$$

Slobodna grupa naziv je dobila upravo po tome jer njezina prezentaciju nema relacija.

Spomenimo sada nekoliko riječi o označavanju prezentacija. Obično, relacije u prezentacijama zapisujemo kao jednadžbe. Stoga, relacije:

$$a^3, b^2, aba^{-1}b^{-1}$$

možemo također zapisati kao:

$$a^3 = 1, b^2 = 1, ab = ba.$$

Definicija 6.6. *Grupa G je **konačno generirana** ako ima prezentaciju $(X \mid R)$, pri čemu je X konačni skup. Grupu G nazivamo **konačno prezentirana** ako ima prezentaciju $(X \mid R)$, pri čemu su i X i R konačni.*

Sada ćemo definirati tip grupe koji ćemo kasnije povezati sa prezentacijama.

Definicija 6.7. *Grupa G je **tipa** $\mathbb{T}(x, y \mid x^{2^{n-1}}, yxy^{-1}x, y^{-2}x^{2^{n-2}})$ ako je $n \geq 2$ i G je generirana sa dva elementa a i b takva da vrijedi:*

$$a^{2^{n-1}} = 1,\ bab^{-1} = a^{-1} \quad i \quad b^2 = a^{2^{n-2}}.$$

Ove grupe koriste se za definiciju generaliziranih grupa kvaterniona. Prema tome, grupa kvaterniona koju ćemo kasnije definirati pomoću Definicije 6.10 jest tog tipa.

Nakon što smo definirali prezentacije, označavanje tipa grupe iz Definicije 6.7 možemo generalizirati na sljedeći način.

Definicija 6.8. *Neka je F slobodna grupa s bazom X i neka je $R \subseteq F$. Grupa G je **tipa** $\mathbb{T}(X \mid R)$ ako postoji surjektivni homomorfizam $\varphi : F \to G$ definiran sa $\varphi(r) = 1$, $\forall r \in R$.*

Grupa G sa prezentacijom $G = (X \mid R)$ očito je tipa $\mathbb{T}(X \mid R)$, ali obrat ne vrijedi. Na primjer, trivijalna grupa $\{1\}$ je tipa $\mathbb{T}(X \mid R)$ za svaki uređeni par $(X \mid R)$. Sljedeći teorem daje vezu između prezentacija i tipova.

Teorem 6.9. ***(von Dyck-ov teorem)***

(i) *Ako grupe G i H imaju prezentacije:*

$$G = (X \mid R) \quad i \quad H = (X \mid R \cup S),$$

tada je H kvocijent od G. Posebno, ako je H grupa tipa $\mathbb{T}(X \mid R)$, tada je H kvocijent od G.

(ii) *Neka je $G = (X \mid R)$ i neka je H grupa tipa $\mathbb{T}(X \mid R)$. Ako je G konačna i $|G| = |H|$, tada je $G \cong H$.*

Dokaz.

(i) Neka je F slobodna grupa s bazom X. Ako je N normalna podgrupa od F generirana sa R i K je normalna podgrupa generirana sa $R \cup S$, tada je $N \subseteq K$.
Prema Teoremu 1.12, funkcija $\psi : F/N \to F/K$ zadana pridruživanjem $\psi : fN \mapsto fK$ je surjektivni homomorfizam. Odnosno, $\operatorname{Ker}\psi = K/N$ iz čega slijedi da je:

$$(F/N)/(K/N) \cong F/K.$$

Prema tome, slijedi da je $H = F/K$ kvocijent od $G = F/N$. Posebno, za H kažemo da je tipa $\mathbb{T}(X \mid R)$ ako H zadovoljava sve relacije sadržane u G.

(ii) U ovom dijelu dokaza koristit ćemo **Dirichletov princip** ili **princip pretinaca** koji kaže: Funkcija $f : X \to X$ na konačnom skupu X je injekcija ako i samo ako je surjekcija. S obzirom da je G konačna, Dirichletov princip kaže da je surjektivni homomorfizam $\psi : G \to H$ iz dijela **(i)** izomorfizam.

□

Uočimo, ako je $G = (X \mid R)$ konačna grupa, tada iz Teorema 6.9 slijedi da je $|G| \geq |H|$ za svaku grupu H tipa $\mathbb{T}(X \mid R)$.

Sada ćemo proučiti prezentacije dviju grupa, **grupe kvaterniona** i **diedralne grupe**.

Irski matematičar W. R. Hamilton (1805. - 1865.) otkrio je $\mathbb{R}$-algebru (vektorski prostor nad $\mathbb{R}$ koji je također i prsten) te je, s obzirom da je dimenzije 4, nazvao *kvaternioni*. Grupa kvaterniona sastoji se od osam posebnih elemenata iz tog sustava.

Definicija 6.10. ***Grupa kvaterniona*** *je grupa* $\boldsymbol{Q}$ *reda* 8 *koja se sastoji od sljedećih matrica u* $GL(2, \mathbb{C})$*:*

$$\boldsymbol{Q} = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\},$$

pri čemu je I jedinična matrica, $A = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ *i* $B = \left[\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right]$.

Element $A \in \mathbb{Q}$ je reda 4 pa je stoga $\langle A \rangle$ podgrupa reda 4, indeksa 2. Drugi skup je $B\langle A \rangle = \{B, BA, BA^2, BA^3\}$. Uočimo da vrijedi: $B^2 = A^2$ i $BAB^{-1} = A^{-1}$.

Propozicija 6.11. *Za svaki* $n \geq 3$ *postoji generalizirana grupa kvaterniona* Q_n*: grupa sa sljedećom prezentacijom reda* 2^n*:*

$$Q_n = (a, b \mid a^{2^{n-1}} = 1, bab^{-1} = a^{-1}, b^2 = a^{2^{n-2}})$$

Dokaz.
Ciklička podgrupa $\langle a \rangle$ u Q_n je najviše reda 2^{n-1}, jer je $a^{2^{n-1}} = 1$. Relacija $bab^{-1} = a^{-1}$ povlači da je $\langle a \rangle \trianglelefteq Q_n = \langle a, b \rangle$, pa je $Q_n/\langle a \rangle$ generirana sa slikom od b.
Konačno, relacija $b^2 = a^{2^{n-2}}$ pokazuje da je $|Q_n/\langle a \rangle| \leq 2$. Stoga vrijedi:

$$|Q_n| \leq |\langle a \rangle||Q_n/\langle a \rangle| \leq 2^{n-1} \cdot 2 = 2^n.$$

Obrnutu nejednakost dokazujemo konstruirajući konkretnu grupu H_n tipa:

$$\mathbb{T}(x, y \mid x^{2^{n-1}}, yxy^{-1}x, y^{-2}x^{2^{n-2}}).$$

Promotrimo kompleksne matrice $A = \left[\begin{smallmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{smallmatrix}\right]$ i $B = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, pri čemu je ω primitivni 2^{n-1}-i korijen jedinice i definiramo grupu $H_n = \langle A, B \rangle \subseteq GL(2, \mathbb{C})$.

Tvrdimo da A i B zadovoljavaju tražene relacije.

Za svaki $i \geq 1$,

$$A^{2^i} = \begin{bmatrix} \omega^{2^i} & 0 \\ 0 & \omega^{-2^i} \end{bmatrix},$$

tako da je $A^{2^{n-1}} = I$ i doista, A je reda 2^{n-1}. Štoviše:

$$B^2 = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right] = A^{2^{n-2}} \quad i \quad BAB^{-1} = \left[\begin{smallmatrix} \omega^{-1} & 0 \\ 0 & \omega \end{smallmatrix}\right] = A^{-1}.$$

Uočimo da A i B ne komutiraju, stoga $B \notin \langle A \rangle$ i skupovi $\langle A \rangle$ i $B\langle A \rangle$ su različiti. S obzirom da je A reda 2^{n-1}, slijedi da je:

$$|H_n| \geq |\langle A \rangle \cup B\langle A \rangle| = 2^{n-1} + 2^{n-1} = 2^n.$$

Prema Teoremu 6.9, $2^n \leq |H_n| \leq |Q_n| \leq 2^n$. Dakle, $|Q_n| = 2^n$ i iz Teorema 6.9(ii) slijedi:

$$Q_n \cong H_n.$$

□

Sljedeća definicija potrebna nam je za definiranje **diedralne grupe.**

Definicija 6.12. *Neka je* $A = \left[\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right]$ *i* $B = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$*, pri čemu je* $\zeta = e^{2\pi i/n}$ *primitivni n-ti korijen jedinice. Definiramo grupu G kao grupu generiranu matricama A i B, odnosno* $G = \langle A, B \rangle$*. Tada vrijedi:*

$$G = \{B^i A^j \mid 0 \leq i \leq 1, 0 \leq j < n\}$$

Uočimo da vrijedi $|G| = 2n$.

Definicija 6.13. ***Diedralna grupa*** D_{2n} *je grupa simetrija pravilnog n-terokuta koja ima dva generatora: rotaciju i osnu simetriju.*

Pravilni n-terokut se prirodno smještava na jediničnu kružnicu u kompleksnoj ravnini. Rotacija je realizirana djelovanjem matrice A iz Definicije 6.12, a osna simetrija djelovanjem matrice B. Zbog toga je D_{2n} izomorfna grupi G iz Definicije 6.12.

Propozicija 6.14. *Diedralna grupa* D_{2n} *ima prezentaciju:*

$$D_{2n} = (a, b \mid a^n = 1, b^2 = 1, bab = a^{-1}).$$

Dokaz.
Neka je C_{2n} grupa definirana sa prethodnom prezentacijom. Prema Teoremu 6.9, vrijedi sljedeće:

$$|C_{2n}| \geq |D_{2n}| = 2n.$$

Dokažimo i obrnutu nejednakost. Ciklička podgrupa $\langle a \rangle$ u C_{2n} je najviše reda n, jer je $a^n = 1$. Relacija $bab^{-1} = a^{-1}$ povlači da je $\langle a \rangle \trianglelefteq C_{2n} = \langle a, b \rangle$, tako da je $C_{2n}/\langle a \rangle$ generirana sa slikom od b. Konačno, relacija $b^2 = 1$ pokazuje da je $|C_{2n}/\langle a \rangle| \leq 2$. Stoga vrijedi:

$$|C_{2n}| \leq |\langle a \rangle||C_{2n}/\langle a \rangle| \leq 2n \quad i \quad |C_{2n}| = 2n.$$

Dakle, iz Teorema 6.9 (ii) slijedi:

$$C_{2n} \cong D_{2n}.$$

□

Za kraj, proučit ćemo tvrdnju koja se odnosi na svojstvo neabelove grupe reda 6 no najprije iskažimo tvrdnje i definicije koje su potrebne za njezino razumijevanje.

Teorem 6.15. ***(Lagrange-ov teorem)***
Ako je H podgrupa konačne grupe G, tada je $|H|$ djelitelj od $|G|$. Drugim riječima, postoji broj $t > 0$ takav da je $|G| = t|H|$.

Dokaz ovog teorema nalazi se u [1] na 35. stranici.

Definicija 6.16. *Neka je G grupa i H njezina podgrupa.* ***Indeks*** *od H u G je broj lijevih (odnosno broj desnih) podskupova od H u G. Označavamo ga sa $[G : H]$.*

Indeks $[G : H]$ je broj t u formuli $|G| = t|H|$ iz Teorema 6.15 takav da vrijedi:

$$|G| = [G : H]|H|.$$

Ova formula pokazuje da je indeks $[G : H]$ također djelitelj od $|G|$. Štoviše, vrijedi:

$$[G : H] = |G|/|H|.$$

Propozicija 6.17. *Neka je H podgrupa grupe G indeksa 2. Tada vrijedi:*

(i) $g^2 \in H$ *za svaki* $g \in G$

(ii) $H \trianglelefteq G$

Iskažimo sada i dokažimo prethodno spomenutu tvrdnju.

Propozicija 6.18. *Ako je G neabelova grupa reda 6, tada je $G \cong S_3$.*

Dokaz. Prema Teoremu 6.15, elementi grupe G različiti od neutralnog elementa mogu biti reda 2, 3 ili 6. Međutim, ukoliko grupa sadrži element reda 6 tada je ona ciklička iz čega slijedi da mora biti Abelova što je u kontradikciji s pretpostavkom propozicije. Prema tome, G mora sadržavati neki element a reda 3 i element b reda 2.

S obzirom da je $\langle a \rangle$ grupa indeksa 2, prema Propoziciji 6.17 (ii) slijedi da je $\langle a \rangle \trianglelefteq G$ pa mora vrijediti da je $bab^{-1} = a$ ili $bab^{-1} = a^{-1}$. Prvu mogućnost odbacujemo jer G nije Abelova grupa. Prema tome, G je tipa $\mathbb{T}(a, b \mid a^3, b^2, bab = a^{-1})$ pa iz Teorema 6.9 (ii) slijedi da je $D_6 \cong G$, odnosno $D_6 \cong S_3$. □

Bibliografija

[1] Rotman J. J., *Advanced Modern Algebra. Graduate Studies in Mathematics*, sv. 114, American Mathematical Society, Providence, RI, (2010.).

[2] Hungerford T. W., *Algebra, Graduate Text in Mathematics*, sv. 73, (Springer, Verlag, New York, 1980), Reprint of the 1974 original.

Sažetak

Tema ovog diplomskog rada su slobodne grupe i prezentacije. U uvodnom poglavlju definirani su osnovni pojmovi povezani sa grupom te preslikavanja među njima. Nakon toga definiran je pojam kategorija te navedeno nekoliko primjera kategorija, između ostalih i kategorija grupa koja nam je od posebne važnosti za ovaj rad. Definirali smo slobodne objekte u konkretnoj kategoriji. Posebno, slobodne grupe definirali smo kao slobodni objekt nad nekim skupom X u kategoriji grupa. Nakon definiranja pojmova riječ, inverz neprazne riječi, podriječ te reducirana riječ, pokazali smo da skup svih reduciranih riječi sa operacijom izravnog dopisivanja i elementarnog skraćivanja odgovara pojmu slobodne grupe sa bazom X. Zatim smo naveli najvažnije rezultate povezane uz pojam slobodne Abelove grupe koji su nam bili potrebni za kasnije razumijevanje sadržaja rada. Prethodno definiranu slobodnu Abelovu grupu i komutatorsku podgrupu povezali smo sa slobodnom grupom te smo definirali njezin rang. Tema posljednjeg poglavlja su prezentacije. Tu je pokazana tvrdnja da svaka grupa ima prezentaciju te navedeno nekoliko primjera prezentacija, poput primjerice prezentacija grupe kvaterniona i diedralne grupe.

Summary

Theme of this thesis are free groups and presentations. In introduction we defined basic terms related to groups and mappings between them. We defined the term category and showed several examples, the most important one being the category of groups. We defined what a free object in a concrete category is. Especially, we defined a free group as a free object on set X in category of groups. After that, we defined the terms: word, the inverse of a nonempty word, a subword and a reduced word and we have shown that set of all reduced words with operations juxtaposition and elementary cancellation is equivalent to the term free group with basis X. We mentioned the most important results related to free Abelian groups needed for this thesis. Previously defined free Abelian groups and commutator subgroups are connected with free groups and their rank is defined. In the last chapter we showed that every group has a presentation and mentioned several examples of presentations such as a presentation of the group of quaternions and dihedral group.

Životopis

Rođena sam 05.09.1990. godine u Koprivnici. 1997. godine upisana sam u Osnovnu školu Veliki Bukovec. 2005. godine upisujem Prvu gimnaziju Varaždin, smjer prirodoslovno-matematički. Po završetku gimnazije, 2009. godine upisujem sveučilišni preddiplomski studij matematike (smjer nastavnički) na Prirodoslovno-matematičkom fakultetu u Zagrebu. 2013. godine stječem akademski naziv sveučilišna prvostupnica (baccalaurea) edukacije matematike. Iste godine i na istom fakultetu upisujem sveučilišni diplomski studij matematike, također smjer nastavnički, koji završavam 2015. godine.