Nielsen-Schreierov teorem

Semren, Matea

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Matea Semren

NIELSEN-SCHREIEROV TEOREM

Diplomski rad

Voditelj rada:
prof. dr. sc. Ozren Perše

Zagreb, rujan, 2014.

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

Nielsen-Schreierov teorem je jedan od fundamentalnih rezultata o slobodnim grupama. Postoji više dokaza ovog teorema. Prvi dokaz je dao J. Nielsen 1921. za konačnogenerirane podgrupe. Pretpostavku o konačnosti uklonio je O. Schreier 1926. Drugi način dokaza su dali R. Baer i F. Levi 1933. U ovom radu obradit ćemo dokaz A. J. Weira.
Najprije ćemo se upoznati s osnovnim pojmovima i rezultatima iz teorije grupa, a zatim sa slobodnim grupama. Rad je podijeljen na dva dijela.
U prvom dijelu rada upoznat ćemo se s pojmom grupe, podgrupe, generiranom grupom, normalnom podgrupom kao navažnijom klasom podgrupa, te kvocijentnim grupama koje nam govore kako iz već postojećih grupa konstruirati nove grupe. Također, pokazat ćemo kako uspostaviti odnos između dvije grupe preko homomorfizama, te u skladu s tim obraditi tri teorema o izomorfizmima.
U drugom ćemo dijelu najprije reći nešto o direktnoj sumi Abelovih grupa, te zatim preko direktne sume definirati slobodne Abelove grupe. Zatim ćemo definirati rang slobodne Abelove grupe, te dati karakterizaciju slobodnih Abelovih grupa koja će nam biti motivacija za općenitu definiciju slobodne grupe. Pokazat ćemo kako konstruirati slobodnu grupu iz proizvoljnog skupa elemenata. Uspostavit ćemo vezu između slobodnih grupa i grupa općenito, te definirati prezentaciju grupe. Zatim ćemo definirati transverzalu, te izdvojiti Schreierovu transverzalu preko koje ćemo dokazati Nielsen-Schreierov teorem, koji kaže da je svaka podgrupa slobodne grupe također slobodna grupa. Na kraju ćemo navesti nekoliko posljedica Nielsen-Schreierovog teorema. Kao jednu od tih posljedica Nielsen-Schreierovog teorema, prezentiramo dokaz činjenice da je podgrupa konačnog indeksa konačnogenerirane slobodne grupe također konačnogenerirana.

Poglavlje 1

Grupe

Grupa, kao algebarska struktura, je jedan od najvažnijih pojmova u matematici. Grupe se pojavljuju u analizi, algebri, teoriji brojeva, algebarskoj geometriji i drugim granama matematike.

1.1 Grupe i podgrupe

Da bismo definirali grupu potrebno je definirati binarnu operaciju.

Definicija 1.1.1. *Neka je G neprazan skup. Binarna operacija na skupu G je funkcija*

$$\cdot : G \times G \to G.$$

Osnovni primjeri binarne operacije su zbrajanje $(x, y) \to x + y$ i množenje $(x, y) \to xy$ na skupu $\mathbb{R}$, kompozicija funkcija $(f, g) \to f \circ g$ itd.

Definicija 1.1.2. *Neka je G neprazan skup i $\cdot$ binarna operacija na G. Kažemo da je $(G, \cdot)$ grupa ako vrijedi:*

(i) zakon asocijativnosti: za svaki $x, y, z \in G$ vrijedi

$$(x \cdot y) \cdot z = x \cdot (y \cdot z),$$

(ii) postoji neutralni element $e \in G$, tj. takav da za svaki $x \in G$ vrijedi

$$x \cdot e = e \cdot x = x,$$

(iii) za svaki $x \in G$ postoji inverzni element $x^{-1} \in G$, tj. takav da vrijedi

$$x \cdot x^{-1} = x^{-1} \cdot x = e.$$

Ako još vrijedi zakon komutativnosti, tj. $x \cdot y = y \cdot x$ za svaki $x, y \in G$, kažemo da je G komutativna ili Abelova grupa. U suprotnom kažemo da je G nekomutativna grupa.

Osim podjele na komutativne i nekomutativne grupe, grupe možemo dijeliti na konačne i beskonačne.

Definicija 1.1.3. *Neka je G grupa. Red grupe G definiramo kao $|G| = card(G)$, tj. red grupe G je kardinalni broj skupa G.*
Ako je $|G| < \infty$ kažemo da je G konačna grupa. Inače kažemo da je G beskonačna.

Lako se vidi da je skup $\mathbb{Z}$ (Abelova) grupa uz binarnu operaciju zbrajanja. Također se može vidjeti da su skupovi $\mathbb{Q}$ i $\mathbb{R}$ (Abelove) grupe uz binarnu operaciju zbrajanja, a skupovi $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$ i $\mathbb{R}^{\times} = \mathbb{R} \setminus \{0\}$ su grupe uz operaciju množenja. Primijetimo da $\mathbb{Z}$ nije grupa uz množenje, jer ne postoji inverzni element niti za jedan element iz $\mathbb{Z}$ osim za 1 i -1.
U sljedećoj lemi navodimo neka osnovna svojstva grupe.

Lema 1.1.4. *Neka je $(G, \cdot)$ grupa. Vrijede sljedeća svojstva.*

(i) Neka su $a, b, x \in G$. Ako je $a \cdot x = b \cdot x$ ili $x \cdot a = x \cdot b$, tada je $a = b$.

(ii) Neutralni element $e \in G$ je jedinstven.

(iii) Za svaki $x \in G$ postoji jedinstven inverzni element koji označavamo s x^{-1}.

(iv) Za svaki $x \in G$ vrijedi $(x^{-1})^{-1} = x$.

Dokaz. (i) Neka su $a, b, x \in G$ takvi da je $x \cdot a = x \cdot b$, $e \in G$ neutralni element, te $x_1 \in G$ takav da je $x \cdot x_1 = x_1 \cdot x = e$. Tada je

$$a = e \cdot a = (x_1 \cdot x) \cdot a = x_1 \cdot (x \cdot a) = x_1 \cdot (x \cdot b) = (x_1 \cdot x) \cdot b = e \cdot b = b.$$

Analogno se dokazuje za $a \cdot x = b \cdot x$.

(ii) Pretpostavimo da neutralni element nije jedinstven. Neka su $e_1, e_2 \in G$ takvi da je

$$e_1 \cdot x = x \cdot e_1 = x \quad \text{i} \quad e_2 \cdot x = x \cdot e_2 = x$$

za svaki $x \in G$. Iz $e_1 \in G$ slijedi $e_1 \cdot e_2 = e_1$, a iz $e_2 \in G$ slijedi $e_1 \cdot e_2 = e_2$. Dakle, $e_1 = e_1 \cdot e_2 = e_2$.

(iii) Neka je $x \in G$. Pretpostavimo da inverzni element od x nije jedinstven, tj. neka su $x_1, x_2 \in G$ takvi da je

$$x_1 \cdot x = x \cdot x_1 = e \quad \text{i} \quad x_2 \cdot x = x \cdot x_2 = e.$$

Slijedi da je $x_1 = x_1 \cdot e = x_1 \cdot (x \cdot x_2) = (x_1 \cdot x) \cdot x_2 = e \cdot x_2 = x_2$. Dakle, inverzni element od x je jedinstven.

(iv) Po definiciji inverznog elementa je

$$(x^{-1})^{-1} \cdot x^{-1} = e = x^{-1} \cdot (x^{-1})^{-1} \quad \text{i}$$

$$x^{-1} \cdot x = e = x \cdot x^{-1}.$$

Prema (iii) slijedi da je $(x^{-1})^{-1} = x$.

□

Definicija 1.1.5. *Proizvoljan podskup A grupe G naziva se kompleks. Za proizvoljne A, B definiramo produkt kompleksa*

$$AB := \{ab : a \in A, b \in B\}.$$

Posebno, ako je $B = \{x\}$, pisat ćemo kraće Ax.

Intuitivno, kompleks $H \subseteq G$ je podgrupa grupe G ako je i sam grupa. Npr. $\mathbb{Q}$ je podgrupa grupe $\mathbb{R}$ (uz operaciju zbrajanja).
Sada ćemo dati formalnu definiciju podgrupe.

Definicija 1.1.6. *Podskup H grupe G je podgrupa, u oznaci $H \leq G$, ako vrijede sljedeća svojstva:*

(i) $e \in H$,

(ii) ako je $x, y \in H$, *onda je* $x \cdot y \in H$,

(iii) ako je $x \in H$, *onda je* $x^{-1} \in H$.

U nastavku ćemo (ako nije potrebno naglasiti o kojoj je binarnoj operaciji riječ) umjesto $x \cdot y$ pisati xy.
Sljedeći rezultat je tzv. *kriterij podgrupe*.

Propozicija 1.1.7. *Kompleks $H \subseteq G$ je podgrupa grupe G ako i samo ako za svaki $x, y \in H$ vrijedi $xy^{-1} \in H$.*

Dokaz. Neka je H podgrupa od G, te $x, y \in H$. Tada je i $y^{-1} \in H$, pa je $xy^{-1} \in H$.
Obratno, neka je za svaki $x, y \in H, xy^{-1} \in H$. Dokažimo da je H podgrupa. Neka su $x, y \in H$. Prema pretpostavci je $e = xx^{-1} \in H$, te je stoga i $y^{-1} = ey^{-1} \in H$. Slijedi da je i $xy = x(y^{-1})^{-1} \in H$. □

Propozicija 1.1.8. *Neka je $\{H_i\}_{i \in I}$ familija podgrupa grupe G. Tada je $\bigcap_{i \in I} H_i$ također podgrupa grupe G.*

Dokaz. Neka je $H = \bigcap_{i \in I} H_i$. Ako je $x, y \in H$, tada je $x, y \in H_i$, za svaki $i \in I$. Budući da su H_i podgrupe grupe G, prema propoziciji 1.1.7 je $xy^{-1} \in H_i$, za svaki $i \in I$. Slijedi da je $xy^{-1} \in H$. Prema istoj propoziciji slijedi da je H podgrupa grupe G. $\square$

Prethodna propozicija nam omogućuje sljedeću definiciju.

Definicija 1.1.9. *Za proizvoljan podskup S grupe G, definiramo*

$$\langle S \rangle := \bigcap_{\substack{H < G \\ S \subseteq G}} H.$$

To je (prema prethodnoj propoziciji) podgrupa grupe G, koju zovemo grupa generirana skupom S; sam skup S zovemo skup generatora.
Kažemo da je grupa G konačnogenerirana ako postoji konačan skup $S = \{x_1, ..., x_n\}$ takav da je $G = \langle S \rangle$ i u tom slučaju pišemo $G = \langle x_1, ...x_n \rangle$. Grupa G je ciklička ako se može generirati jednim elementom, tj. ako postoji $g \in G$ takav da je $G = \langle g \rangle$. Svaki takav g se zove generator cikličke grupe G.

Potpoglavlje završavamo s definicijom komutatorske podgrupe koja je primjer generirane grupe.

Definicija 1.1.10. *Neka je G proizvoljna grupa. Za $x, y \in G$ definiramo njihov komutator*

$$[x, y] := xyx^{-1}y^{-1} \in G.$$

Podgrupa

$$G' = \langle [x, y] : x, y \in G \rangle$$

se zove komutatorska podgrupa grupe G.

1.2 Homomorfizmi, normalna podgrupa i kvocijentne grupe

U prethodnom potpoglavlju definirali smo grupu i naveli neka svojstva grupa. Sada nas zanima kako uspostaviti odnos između dvije grupe, tj. kako usporediti dvije grupe. To ćemo napraviti preslikavanjem između njih, točnije, preko homomorfizama.

Definicija 1.2.1. *Neka su G i H dvije grupe. Preslikavanje $f : G \to H$ je homomorfizam ako vrijedi*

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

Homomorfizam f koji je i injekcija naziva se monomorfizam, f koji je i surjekcija naziva se epimorfizam, a f koji je i bijekcija naziva se izomorfizam.
Kažemo da su dvije grupe G i H izomorfne, u oznaci $G \cong H$, ako postoji izomorfizam $f : G \to H$.

Lema 1.2.2. *Neka je $f : G \to H$ homomorfizam. Tada vrijedi:*

(i) $f(e_G) = e_H$,

(ii) $f(x^{-1}) = f(x)^{-1}$.

Dokaz. (i)

$$e_G e_G = e_G \Rightarrow f(e_G)f(e_G) = f(e_G) \Rightarrow$$
$$\Rightarrow f(e_G)f(e_G)f(e_G)^{-1} = f(e_G)f(e_G)^{-1} \Rightarrow f(e_G) = e_H.$$

(ii) Iz $e_G = xx^{-1}$ slijedi $e_H = f(xx^{-1}) = f(x)f(x^{-1})$. Dakle, $f(x^{-1}) = f(x)^{-1}$.

□

Definicija 1.2.3. *Za homomorfizam $f : G \to H$, definiramo jezgru i sliku od f s*

$$\operatorname{Ker} f = \{x \in G : f(x) = e_H\}$$

$$\operatorname{Im} f = \{h \in H : h = f(x),\ \textit{za neki } x \in G\}.$$

Sljedeća lema i propozicija daju nam neka svojstva homomorfizama.

Lema 1.2.4. *Neka su $f : G \to H$ i $g : H \to K$ homomorfizmi grupa. Tada je njihova kompozicija $g \circ f : G \to K$ također homomorfizam grupa. Štoviše, ako su g, h oba monomorfizmi (epimorfizmi, izomorfizmi), onda je $g \circ f$ monomorfizam (epimorfizam, izomorfizam).*

Dokaz. Za $x, y \in G$ imamo

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y).$$

Ovdje smo koristili definiciju kompozicije funkcija i činjenicu da su g i f homomorfizmi. Druga tvrdnja slijedi iz činjenice da je kompozicija dvije injekcije (surjekcije, bijekcije) ponovno injekcija (surjekcija, bijekcija). $\square$

Propozicija 1.2.5. *Neka je $f : G \to H$ homomorfizam. Vrijede sljedeća svojstva.*

(i) $\mathrm{Ker}\, f$ *je podgrupa grupe G, a* $\mathrm{Im}\, f$ *je podgrupa grupe H.*

(ii) Ako je $x \in \mathrm{Ker}\, f$ i $a \in G$, onda je $axa^{-1} \in \mathrm{Ker}\, f$.

(iii) Homomrfizam f je injekcija ako i samo ako je $\mathrm{Ker}\, f = \{e_G\}$.

Dokaz. (i) Da bismo dokazali da je $\mathrm{Ker}\, f$ podgrupa grupe G, prema *kriteriju podgrupe* je dovoljno dokazati da iz $x, y \in \mathrm{Ker}\, f$ slijedi da je $xy^{-1} \in \mathrm{Ker}\, f$, tj. da je $f(xy^{-1}) = 1$. Imamo da je

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e_H e_H = e_H.$$

Ovdje smo koristili definiciju homomorfizma, te (u trećoj jednakosti) lemu 1.2.2 (ii). Analogno dokazujemo za $\mathrm{Im}\, f$. Neka su $y_1, y_2 \in \mathrm{Im}\, f$. Tada postoje $x_1, x_2 \in G$ takvi da je $y_1 = f(x_1)$ i $y_2 = f(x_2)$, pa je

$$y_1 y_2^{-1} = f(x_1)f(x_2)^{-1} = f(x_1)f(x_2^{-1}) = f(x_1 x_2^{-1}).$$

Budući da je $x_1 x_2^{-1} \in G$, slijedi da je $y_1 y_2^{-1} \in \mathrm{Im}\, f$. Dakle, $\mathrm{Im}\, f$ je podgrupa grupe H.

(ii) Neka je $x \in \mathrm{Ker}\, f$ i $a \in G$. Tada je

$$f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)e_H f(a)^{-1} = f(a)f(a)^{-1} = e_H.$$

Slijedi da je $axa^{-1} \in \mathrm{Ker}\, f$.

(iii) Neka je $\mathrm{Ker}\, f = \{e_G\}$, te $x, y \in G$ takvi da je $f(x) = f(y)$. Množenjem s $f(y)^{-1}$ dobivamo

$$e_H = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}).$$

Dakle, $xy^{-1} \in \mathrm{Ker}\, f$. Iz $\mathrm{Ker}\, f = \{e_G\}$ slijedi da je $xy^{-1} = e_G$, odnosno $x = y$. Stoga je f injekcija.

Obratno, neka je f injekcija. Budući da je $f(e_G) = e_H$, iz definicije injekcije slijedi da je $\mathrm{Ker}\, f = \{e_G\}$.

$\square$

Sljedeću lemu ćemo koristi kasnije u dokazu Nielsen-Schreierovog teorema.

Lema 1.2.6. *Neka su Y i S grupe, a $\varphi : Y \to S$ i $\theta : S \to Y$ homomorfizmi takvi da je $\varphi\theta = 1_S$. Tada vrijede sljedeće tvrdnje.*

(i) Neka je preslikavanje $\rho : Y \to Y$ definirano s $\rho = \theta\varphi$. Tada je $\rho\rho = \rho$ i $\rho(a) = a$ za svaki $a \in \operatorname{Im}\theta$.

(ii) Neka je K normalna podgrupa grupe Y generirana skupom $\{y^{-1}\rho(y) : y \in Y\}$. Tada je $K = \operatorname{Ker}\varphi$.

Dokaz. (i) Vrijedi da je

$$\rho\rho = (\theta\varphi)(\theta\varphi) = \theta(\varphi\theta)\varphi = \theta\varphi = \rho.$$

Neka je $a \in \operatorname{Im}\theta$. Tada postoji $b \in S$ takav da je $a = \theta(b)$. Slijedi da je

$$\rho(a) = (\theta\varphi)(a) = (\theta\varphi)(\theta(b)) = \theta((\varphi\theta)(b)) = \theta(b) = a.$$

(ii) Pokažimo da za svaki generator vrijedi $y^{-1}\rho(y) \in \operatorname{Ker}\varphi$. Imamo da je

$$\begin{aligned}\varphi(y^{-1}\rho(y)) = \varphi(y^{-1})\varphi((\theta\varphi)(y)) = \varphi(y)^{-1}(\varphi\theta)\varphi(y) = \\ = \varphi(y)^{-1}\varphi(y) = e_S.\end{aligned}$$

Slijedi da je $K \subseteq \operatorname{Ker}\varphi$.
Da bi smo dokazali obratnu inkluziju, primijetimo da je $\operatorname{Ker}\varphi = \operatorname{Ker}\rho$, jer je θ injekcija, što slijedi iz relacije $\varphi\theta = 1_S$.
Neka je sada $y \in \operatorname{Ker}\varphi = \operatorname{Ker}\rho$. Slijedi da je

$$y = y\rho(y^{-1}) = (y^{-1})^{-1}\rho(y^{-1}) \in K.$$

Dakle, $\operatorname{Ker}\varphi \subseteq K$.

□

U nastavku ćemo definirati *normalne podgrupe*, te pokazati na koji način iz već postojećih grupa konstruirati nove grupe.
Najprije, neka je G grupa, a H neka podgrupa od G. Definiramo jednu relaciju ekvivalencije na $G \times G$ na sljedeći način:

$$\begin{aligned}\forall x, y \in G \quad x \sim y \Leftrightarrow xH = yH \Leftrightarrow x^{-1}y \in H \\ (Hx = Hy \Leftrightarrow yx^{-1} \in H).\end{aligned}$$

Definicija 1.2.7. *Klase na koje se raspada grupa G po relaciji $\sim$ označavamo s xH (tj. Hx) i zovemo lijeve (tj. desne) klase od G po $\sim$. Skup svih lijevih (tj. desnih) klasa od G po $\sim$ označavamo s G/H (tj. $H \setminus G$).*
Ako je $card(G/H) < \infty$, taj broj označavamo s $(G : H)$ i zovemo indeks od H u G.

Definicija 1.2.8. *Neka je G grupa, te $a \in G$. Konjugat od a je svaki element od G oblika*

$$gag^{-1},\ \text{gdje je } g \in G.$$

Definicija 1.2.9. *Podgrupa N grupe G je normalna podgrupa, u oznaci $H \trianglelefteq G$, ako za svaki $n \in N$ i za svaki $g \in G$ vrijedi $gng^{-1} \in N$.*

Primijetimo da je svaka podgrupa komutativne grupe normalna podgrupa. Zbog toga se normalne podgrupe proučavaju samo za nekomutativne grupe.

Lema 1.2.10. *Podgrupa N grupe G je normalna podgrupa ako i samo ako je $gN = Ng$ za svaki $g \in G$. Dakle, svaka desna klasa normalne podgrupe je i lijeva klasa.*

Dokaz. Neka je $N \trianglelefteq G$ i $gn \in gN$. Budući da je N normalna vrijedi da $gng^{-1} \in N$. Neka je $n_1 = gng^{-1}$. Imamo da je $gn = (gng^{-1})g = n_1 g \in Ng$. Dakle, $gN \subseteq Ng$. Za obratnu inkluziju neka je $ng \in Ng$. Budući da je N normalna, vrijedi $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Neka je $n_2 = g^{-1}ng$. Imamo da je $ng = g(g^{-1}ng) = gn_2 \in gN$. Dakle, $gN = Ng$.
Neka je sada $gN = Ng$. Tada za svaki $g \in G$ i za svaki $n \in N$ postoji $n_1 \in N$ takav da je $gn = n_1 g$, tj. $gng^{-1} \in N$ za svaki $g \in G$. Slijedi da je $N \trianglelefteq G$. □

Primjer 1.2.11. *Neka je G grupa, a G' njena komutatorska podgrupa. Pokažimo da je $G' \trianglelefteq G$.*
Trebamo dokazati da je $g\omega g^{-1} \in G'$, za svaki $g \in G$ i za svaki $\omega \in G'$. To je dovoljno dokazati na generatorima, tj. za ω oblika $\omega = [x, y]$ za neke $x, y \in G$. Imamo da je

$$\begin{aligned} g[x,y]g^{-1} &= gxyx^{-1}y^{-1}g^{-1} = \\ &= (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} = \\ &= [gxg^{-1}, gyg^{-1}] \in G'. \end{aligned}$$

Sljedeći teorem, u kojem uvodimo kvocijentne grupe, daje nam način konstrukcije novih grupa iz već postojećih grupa.

Teorem 1.2.12. *Neka je G proizvoljna grupa i $N \trianglelefteq G$. Tada je kvocijentni skup G/N s operacijom*

$$G/N \times G/N \to G/N \quad \text{definiranom s} \quad (xN, yN) \to xyN$$

grupa. Grupa G/N se zove kvocijentna grupa od G po N.
Nadalje, preslikavanje

$$\pi = \pi_N : G \to G/N \quad \textit{definirano s} \quad x \to xN$$

je epimorfizam grupa s jezgrom $\operatorname{Ker} \pi = N$*; π zovemo kanonski epimorfizam ili kanonska surjekcija.*

Dokaz. Prvo ćemo dokazati da je dana operacija množenja dobro definirana. Neka su dani

$$x_1, x_2, y_1, y_2 \in G \quad \text{takvi da je} \quad x_1 N = x_2 N \quad \text{i} \quad y_1 N = y_2 N.$$

To je ekvivalentno s $x_1^{-1} x_2 \in N$ i $y_1^{-1} y_2 \in N$. Želimo dokazati da je $x_1 y_1 N = x_2 y_2 N$, što je ekvivalentno s $y_1^{-1} x_1^{-1} x_2 y_2 \in N$. Budući da je N normalna podgrupa imamo da je

$$y_1^{-1} x_1^{-1} x_2 y_2 = (y_1^{-1}(x_1^{-1} x_2) y_1)(y_1^{-1} y_2) \in N.$$

Dakle, dana operacija je dobro definirana.
Dokažimo sada da je G/N grupa.
Asocijativnost: neka je $xN, yN, zN \in G/N$. Tada je

$$(xNyN)zN = xyNzN = ((xy)z)N = (x(yz))N = xN(yz)N = xN(yNzN).$$

Neutralni element: pokažimo da je N neutralni element. Primijetimo da je $N = eN$. Neka je $xN \in G/N$. Tada je

$$(xN)(eN) = (xe)N = xN.$$

Inverzni element: tvrdimo da je za $xN \in G/N$ inverzni element $x^{-1}N \in G/N$. Imamo da je

$$xNx^{-1}N = (xx^{-1})N = eN = N.$$

Očito je da je π homomorfizam grupa, te da je surjektivan. Naime, za klasu $xN \in G/N$ je $\pi(x) = xN$. Pokažimo još da je $\operatorname{Ker} \pi = N$. Imamo da je

$$\operatorname{Ker} \pi = \{x \in G : xN = e_{G/N} = e_G N = N\} = \{x \in G : x \in N\} = N.$$

□

Poglavlje završavamo s tri osnovna rezultata o homomorfizmima grupa; to su tzv. *Teoremi o izomorfizmima*. Napomenimo da su ovi teoremi fundamentalni rezultati u teoriji grupa.

Teorem 1.2.13. *(Prvi teorem o izomorfizmu)*
Neka je $f : G \to H$ homomorfizam. Tada je $\operatorname{Ker} f \trianglelefteq G$*, a preslikavanje*

$$\varphi : G/\operatorname{Ker} f \to \operatorname{Im} f \quad \textit{definirano s} \quad \varphi(g \operatorname{Ker} f) = f(g)$$

je izomorfizam, tj. $G/\operatorname{Ker} f \cong \operatorname{Im} f$.

Dokaz. Već smo u propoziciji 1.2.5 (ii) vidjeli da je $\operatorname{Ker} f \trianglelefteq G$.
Pokažimo sada da je preslikavanje φ dobro definirano. Neka je $N = \operatorname{Ker} f$. Vrijedi da je

$$aN = bN \Leftrightarrow a^{-1}b \in N \Leftrightarrow f(a^{-1}b) = e_H \Leftrightarrow$$
$$\Leftrightarrow f(a)^{-1}f(b) = e_H \Leftrightarrow \varphi(aN) = f(a) = f(b) = \varphi(bN).$$

Pokažimo sada da je φ izomorfizam. Prvo dokazujemo da je homomorfizam. Imamo da je

$$\varphi(aNbN) = \varphi(abN) = f(ab) = f(a)f(b) = \varphi(aN)\varphi(bN).$$

Surjektivnost: očito je $\operatorname{Im}\varphi \leq \operatorname{Im} f$. Za obratnu inkluziju neka je $y \in \operatorname{Im} f$. Tada postoji $g \in G$ takav da je $y = f(g) = \varphi(gN)$. Slijedi da je $y \in \operatorname{Im}\varphi$. Dakle, $\operatorname{Im}\varphi = \operatorname{Im} f$, tj. φ je surjekcija.
Injektivnost: neka je $\varphi(aN) = \varphi(bN)$. Tada je $f(a) = f(b)$, tj. $e_H = f(a)^{-1}f(b) = f(a^{-1}b)$. Dakle, $a^{-1}b \in N$, odnosno $aN = bN$.
Budući da je φ homomorfizam koji je ujedno i bijekcija, slijedi da je φ izomorfizam. □

Prije drugog teorema o izomorfizmu navodimo sljedeću propoziciju.

Propozicija 1.2.14. *Ako su H i K podgrupe grupe G, te ako je jedna od njih normalna podgrupa, onda je $HK \leq G$ i vrijedi $HK = KH$.*

Dokaz. Pretpostavimo da je $K \trianglelefteq G$. Tvrdimo da je $HK = KH$. Ako je $hk \in HK$, onda je $k_1 = hkh^{-1} \in K$ jer je $K \trianglelefteq G$. Sada imamo da je $hk = hkh^{-1}h = k_1h \in KH$. Slijedi da je $HK \subseteq KH$.
Za obratnu inkluziju, neka je $k_2 = h^{-1}kh \in K$. Tada je $kh = hh^{-1}kh = hk_2 \in HK$. Dakle, $HK = KH$.
Dokažimo sada da je HK podgrupa. Dokazujemo po definiciji.
Neutralni element: budući da su H i K podgrupe, slijedi da je $e \in H$ i $e \in K$, pa je $e = ee \in HK$.
Inverzni element: ako je $hk \in HK$, onda je $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.
Zatvorenost na binarnu operaciju: ako je $h_1k_1, h_2k_2 \in HK$, onda je

$$h_1k_1h_2k_2 \in HKHK = HHKK = HK.$$

□

Teorem 1.2.15. *(Drugi teorem o izomofizmu) Ako su $H, K \leq G$, te $H \trianglelefteq G$, onda je $HK \leq G$, $H \cap K \trianglelefteq K$, te*

$$K/(H \cap K) \cong HK/H.$$

Dokaz. Budući da je $H \trianglelefteq G$, prema prethodnoj propoziciji je $HK \leq G$. Da je $H \trianglelefteq HK$, slijedi iz općenitije činjenice: ako je $H \leq S \leq G$ i $H \trianglelefteq G$, onda je $H \trianglelefteq S$.
Sada pokazujemo da za svaki $xH \in HK/H$ postoji $k \in K$ takav da je $xH = kH$. Primijetimo da je $xH = hkH$, gdje je $h \in H$ i $k \in K$. Imamo da je $hk = kk^{-1}hk = kh'$, gdje je $h' = k^{-1}hk \in H$ jer je H normalna. Dakle, $xH = hkH = kh'H = kH$.
Slijedi da je funkcija $f : K \to HK/H$ definirana s $f(k) = kH$ surjekcija. Štoviše, f je homomorfizam jer je restrikcija prirodnog homomorfizama $\pi : G \to G/H$. Budući da je $\operatorname{Ker} \pi = H$, imamo da je $\operatorname{Ker} f = H \cap K$. Slijedi da je $H \trianglelefteq K$. Prema *Prvom teoremu o izomorfizmu* je

$$K/(H \cap K) \cong HK/H.$$

□

Teorem 1.2.16. *(Treći teorem o izomorfizmu) Ako su H i K normalne podgrupe grupe G, te $K \leq H$, onda je $H/K \trianglelefteq G/K$ i*

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

Dokaz. Definiramo $f : G/K \to G/H$ s $f(gK) = gH$. Primijetimo da je f dobro definirana, jer za $g_1 \in G$ je $g_1K = gK$ ako i samo ako $g^{-1}g_1 \in K \leq H$. Dakle, $g_1H = gH$.
Preslikavanje f je surjektivni homomorfizam. Naime, neka su $a, b \in G$. Tada je

$$f(aKbK) = f(abK) = abH = aHbH = f(aK)f(bK).$$

Očito je f surjekcija.
Iz $\operatorname{Ker} f = \{gK : gH = H\} = \{gK : g \in H\} = H/K$ slijedi da je $H/K \trianglelefteq G/K$. Budući da je f surjekcija po *Prvom teoremu o izomorfizmu* slijedi $(G/K)/(H/K) \cong G/H$ □

Poglavlje 2

Slobodne grupe

2.1 Slobodne Abelove grupe

Već smo ranije spomenuli Abelove grupe. Prisjetimo se, to su grupe za koje vrijedi svojstvo komutativnosti, tj. ako je G Abelova grupa, te $a, b \in G$ tada vrijedi $ab = ba$. U ovom potpoglavlju ćemo definirati slobodnu Abelovu grupu, a u sljedećem potpoglavlju ćemo dati općenitiju definiciju slobodnih grupa.
Najprije ćemo reći nešto direktnoj sumi Abelovih grupa $S_1, ..., S_n$.

Definicija 2.1.1. *Neka su S i T podgrupe Abelove grupe G. Kažemo da je G direktna suma, u oznaci*

$$G = S \oplus T,$$

ako je $S + T = G$ (za svaki $g \in G$ postoje $s \in S, t \in T$ takvi da je $g = s + t$) i $S \cap T = \{0\}$.

Propozicija 2.1.2. *Neka je G Abelova grupa, te $S, T \leq G$. Sljedeće tvrdnje su ekvivalentne.*

(i) $G = S \oplus T$.

(ii) *Svaki $g \in G$ ima jedinstven zapis $g = s + t$, gdje je $s \in S, t \in T$.*

(iii) *Postoje homomorfizmi $p : G \to S$ i $q : G \to T$ zvani projekcije, te $i : S \to G$ i $j : T \to G$ zvani injekcije, takvi da vrijedi*

$$p \circ i = 1_S, \quad q \circ j = 1_T, \quad p \circ j = 0,$$

$$q \circ i = 0, \quad i \circ p + j \circ q = 1_G.$$

Dokaz. $(i) \Rightarrow (ii)$ Po pretpostavci je $G = S \oplus T$, pa svaki $g \in G$ možemo zapisati kao $g = s + t$, gdje je $s \in S, t \in T$. Pokažimo da je taj zapis jedinstven. Pretpostavimo

suprotno, tj. da postoje $s' \in S, t' \in T$ takvi da je $g = s' + t'$. Iz $s + t = s' + t'$ slijedi $s - s' = t - t' \in S \cap T = \{0\}$. Dakle, $s = s', t = t'$.
$(ii) \Rightarrow (iii)$ Ako je $g \in G$, onda postoje jedinstveni $s \in S, t \in T$ takvi da je $g = s + t$. Slijedi da su p i q, definirane s $p(g) = s$ i $q(g) = t$, dobro definirane. Lako se provjeri da su to homomorfizmi, kao i funkcije i i j definirane s $i(s) = s$ i $j(t) = t$. Zatim, imamo da je

$$(p \circ i)(s) = p(i(s)) = p(s) = s \quad \text{i}$$

$$(i \circ p + j \circ q)(g) = i(p(g)) + j(q(g)) = i(s) + j(t) = s + t = g.$$

Na isti način se dokažu i ostale tvrdnje.
$(iii) \Rightarrow (i)$ Ako je $g \in G$, iz jednadžbe $1_G = i \circ p + j \circ q$ slijedi da je

$$g = (i \circ p)(g) + (j \circ q)(g) \in S + T,$$

jer je $S = \operatorname{Im} i$ i $T = \operatorname{Im} j$. □

Proširimo definiciju direktne sume za $n \geq 2$.

Definicija 2.1.3. *Neka su $S_1, ..., S_n$ podgrupe Abelove grupe. Definiramo konačnu direktnu sumu $S_1 \oplus S_2 \oplus ... \oplus S_n$ koristeći indukciju za $n \geq 2$*

$$S_1 \oplus S_2 \oplus ... \oplus S_{n+1} = (S_1 \oplus S_2 \oplus ... \oplus S_n) \oplus S_{n+1}.$$

Propozicija 2.1.4. *Neka su $S_1, ..., S_n$ podgrupe Abelove grupe G takve da je*

$$G = S_1 + ... + S_n,$$

tj. za svaki $g \in G$ postoje $s_i \in S_i$, za svaki $i \leq n$, takvi da je $g = s_1 + ... + s_n$.
Sljedeće tvrdnje su ekvivalente.

(i) $G = S_1 \oplus ... \oplus S_n$.

(ii) *Svaki $g \in G$ ima jedinstven zapis oblika $g = s_1 + ... + s_n$, gdje je $s_i \in S_i$, za svaki $i \leq n$.*

(iii) *Za svaki $i \leq n$ je $S_i \cap (S_1 \oplus ... \oplus S_{i-1} \oplus S_{i+1} \oplus ... \oplus S_n) = \{0\}$.*

Dokaz. $(i) \Rightarrow (ii)$ Dokaz provodimo indukcijom po $n \geq 2$. Bazu nam daje propozicija 2.1.2. Za korak indukcije definiramo

$$T = S_1 \oplus S_2 \oplus ... \oplus S_n.$$

Slijedi da je $G = T \oplus S_{n+1}$. Prema istoj propoziciji, ako je $g \in G$, onda g ima jedinstven zapis oblika $g = t + s_{n+1}$, gdje je $t \in T$ i $s_{n+1} \in S_{n+1}$. Pretpostavka indukcije kaže da t ima

jedinstven zapis $t = s_1 + s_2 + ... + s_n$, gdje je $s_i \in S_i$, za svaki $\leq n$. Dakle, $g = s_1 + s_2 + ... + s_n$.
$(ii) \Rightarrow (iii)$ Pretpostavimo da je $x \in S_i \cap (S_1 \oplus S_2 \oplus ...S_{i-1} \oplus S_{i+1} \oplus ... \oplus S_n)$. Tada je

$$x = s_i \in S_i \quad \text{i} \quad x = \sum_{j \neq i} s_j, \quad \text{tj.} \quad 0 = -s_i + \sum_{j \neq i} s_j.$$

Ali, $0 = 0 + 0 + ... + 0$, pa zbog jedinstvenosti zapisa slijedi da je $s_j = 0$ za svaki $j \leq n$. Dakle, $x = 0$.
$(iii) \Rightarrow (i)$ Budući da je $S_{n+1} \cap (S_1 + S_2 + ... + S_n) = \{0\}$, slijedi da je

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

Prema pretpostavci indukcije je $S_1 + S_2 + ... + S_n = S_1 \oplus S_2 \oplus ... \oplus S_n$, jer za svaki $j \leq n$ imamo

$$S_j \cap (S_1 + ... + S_{j-1} + S_{j+1} + ... + S_n) \subseteq S_j \cap (S_1 + ... + S_{j-1} + S_{j+1} + ... + S_n + S_{n+1}) = \{0\}.$$

□

U definiciji 2.1.1 i definiciji 2.1.3 smo definirali unutarnju direktnu sumu. Postoji još i vanjska direktna suma Abelovih grupa $S_1, ..., S_n$, definirana na Kartezijevom produktu $S_1 \times S_2 \times ... \times S_n$ s binarnom operacijom

$$(s_1, ..., s_n) + (s'_1, ..., s'_n) = (s_1 + s'_1, ..., s_n + s'_n).$$

U sljedećem korolaru ćemo dokazati da su ove dvije direktne sume ekvivalentne.

Korolar 2.1.5. *Neka su S i T podgrupe Abelove grupe G. Ako je $G = S \oplus T$, onda je $S \oplus T \cong S \times T$.*
Obratno, ako su S i T Abelove grupe, definiramo podgrupe $S' \cong S$ i $T' \cong T$ od $S \times T$ na sljedeći način

$$S' = \{(s, 0) : s \in S\},$$
$$T' = \{(0, t) : t \in T\}.$$

Tada je $S \times T = S' \oplus T'$.

Dokaz. Definiramo $f : S \oplus T \to S \times T$ na sljedeći način: ako je $a \in S \oplus T$, tada po propoziciji 2.1.2 element a ima jedinstven zapis $a = s + t$, pa je stoga $f : a \to (s, t)$ dobro definirana funkcija. Pokažimo da je f homomorfizam. Neka je $b = s_1 + t_1 \in S \oplus T$, tada je

$$\begin{aligned} f(a + b) &= f((s + t) + (s_1 + t_1)) = f((s + s_1) + (t + t_1)) = \\ &= (s + s_1, t + t_1) = (s, t) + (s_1, t_1) = \\ &= f(a) + f(b). \end{aligned}$$

Da je preslikavanje f bijekcija slijedi iz jedinstvenosti zapis svakog $a \in S \oplus T$.
Obratno, ako je $a = (s, t) \in S \times T$, onda je $a = (s, 0) + (0, t) \in S' + T'$ i $S' \cap T' = \{(0, 0)\}$.
Dakle, $S \times T = S' \oplus T'$. □

Sada možemo dati definiciju slobodne Abelove grupe.

Definicija 2.1.6. *Neka je $F = \langle x_1, ..., x_n \rangle$ Abelova grupa. Ako je*

$$F = \langle x_1 \rangle \oplus ... \oplus \langle x_n \rangle,$$

gdje je svaki $\langle x_i \rangle \cong \mathbb{Z}$, onda F zovemo (konačnogeneriranom) slobodnom Abelovom grupom s bazom $\{x_1, ..., x_n\}$. Općenitije, svaku grupu izomorfnu s F zovemo slobodnom Abelovom grupom.

Primjer slobodne Abelove grupe je $\mathbb{Z}^m = \mathbb{Z} \times ... \times \mathbb{Z}$.
Želimo definirati rang slobodne Abelove grupe kao broj elemenata baze. Prije toga moramo provjeriti imaju li svake dvije baze slobodne Abelove grupe F jednak broj elemenata.

Propozicija 2.1.7. *Ako su $G_1, ..., G_n$ Abelove grupe i $H_i \leq G_i$, za svaki $i \leq n$, onda je*

$$(G_1 \oplus G_2 \oplus ... \oplus G_n)/(H_1 \oplus H_2 \oplus ... \oplus H_n) \cong (G_1/H_1) \oplus ... \oplus (G_n/H_n).$$

Dokaz. Definiramo $f : G_1 \oplus ... \oplus G_n \to (G_1/H_1) \oplus ... \oplus (G_n/H_n)$ s

$$(g_1, ..., g_n) \to (g_1 + H_1, ..., g_n + H_n).$$

Budući da je f epimorfizam s $\mathrm{Ker}\, f = H_1 \oplus ... \oplus H_n$, tvrdnja slijedi iz *Prvog teorema o izomorfizmu*. □

Propozicija 2.1.8. *Ako je F (konačnogenerirana) slobodna Abelova grupa, onda svake dvije baze od F imaju jednak broj elemenata.*

Dokaz. Ako je $\{x_1, ..., x_n\}$ baza od F, onda je $F \cong \mathbb{Z}^n$. Ako je $\{y_1, ..., y_m\}$ baza od F, onda je $F \cong \mathbb{Z}^m$. Slijedi da je $\mathbb{Z}^n \cong \mathbb{Z}^m$. Pokažimo da mora vrijediti $m = n$.
Iz $\mathbb{Z}^m = \mathbb{Z} \oplus \mathbb{Z} \oplus ... \oplus \mathbb{Z}$ (m-puta) slijedi da je $2\mathbb{Z}^m = 2\mathbb{Z} \oplus ... \oplus 2\mathbb{Z}$. Prema propoziciji 2.1.7 je $\mathbb{Z}^m/2\mathbb{Z}^m \cong (\mathbb{Z}/2\mathbb{Z}) \oplus ... \oplus (\mathbb{Z}/2\mathbb{Z})$. Stoga je $|\mathbb{Z}^m/2\mathbb{Z}^m| = 2^m$.
Budući da $\mathbb{Z}^m \cong \mathbb{Z}^n \Rightarrow \mathbb{Z}^m/2\mathbb{Z}^m \cong (\mathbb{Z}^n/2\mathbb{Z}^n)$, imamo da je $|\mathbb{Z}^m/2\mathbb{Z}^m| = |\mathbb{Z}^n/2\mathbb{Z}^n|$, tj. $2^m = 2^n$.
Slijedi da je $m = n$. □

Sada ima smisla definirati rang.

Definicija 2.1.9. *Ako je F slobodna Abelova grupa s bazom $\{x_1, ..., x_n\}$, onda n nazivamo rang od F, uz oznaku $rang(F) = n$.*

Sljedeći teorem nam daje karakterizaciju slobodnih Abelovih grupa.

Teorem 2.1.10. *Neka je F slobodna Abelova grupa s bazom $X = \{x_1, ..., x_n\}$, G proizvoljna Abelova grupa, te $\gamma : X \to G$ neka funkcija. Tada postoji jedinstven homomorfizam $g : F \to G$ takav da je $g(x_i) = \gamma(x_i)$, za svaki $x_i \in X$.*

Dokaz. Prema propoziciji 2.1.4 (ii), svaki element $a \in F$ ima jedinstven zapis

$$a = \sum_{i=1}^{n} m_i x_i, \text{ gdje je } m_i \in \mathbb{Z}.$$

Definiramo $g : F \to G$ s

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

Ako je $h : F \to G$ homomorfizam takav da vrijedi $h(x_i) = g(x_i)$, za svaki $x_i \in X$, onda je $h = g$. Naime, dva homomorfizma koja se podudaraju na skupu generatora moraju biti jednaka. □

Vrijedi li obrat prethodnog teorema? Potvrdan odgovor daje nam sljedeća propozicija.

Propozicija 2.1.11. *Neka je A Abelova grupa koja sadrži skup $X = \{x_1, ..., x_n\}$, te neka za svaku Abelovu grupa G i svaku funkciju $\gamma : X \to G$ postoji jedinstven homomorfizam $g : A \to G$, takav da je $g(x_i) = \gamma(x_i)$, za svaki $x_i \in X$. Tada je $A \cong \mathbb{Z}^n$, tj. A je slobodna Abelova grupa ranga n.*

Dokaz. Neka su $p : X \to A$ i $q : X \to \mathbb{Z}^n$ inkluzije. Budući da je $\mathbb{Z}^n$ Abelova grupa prema pretpostavci postoji jedinstven homomorfizam $g : A \to \mathbb{Z}^n$ takav da je $g \circ p = q$.
Budući da je $\mathbb{Z}^n$ je slobodna Abelova grupa, prema teoremu 2.1.10 postoji jedinstven homomorfizam $h : \mathbb{Z}^n \to A$ takav da je $h \circ q = p$.
Tvrdimo da je g izomorfizam. Vrijedi da je $h \circ g \circ p = h \circ q = p$. Prema pretpostavci je $h \circ g$ jedinstven takav homomorfizam. Ali, 1_A je isto takav homomorfizam, pa slijedi da je $h \circ g = 1_A$. Analogno se pokaže da je $g \circ h = 1_{Z^n}$. Stoga je g izomorfizam. □

2.2 Slobodne grupe

U prethodnom potpoglavlju su nam teorem 2.1.10 i propozicija 2.1.11 dali karakterizaciju slobodnih Abelovih grupa, te su nam motivacija za sljedeću definiciju.

Definicija 2.2.1. *Neka je F grupa i $X \subseteq F$. Kažemo da je F slobodna grupa s bazom X ako za svaku grupu G i svaku funkciju $f : X \to G$ postoji jedinstven homomorfizam $\varphi : F \to G$ takav da je $\varphi(x) = f(x)$, za svaki $x \in X$.*

Postavlja se pitanje postoji li (ne-abelova) slobodna grupa. Postojanje slobodne grupe ćemo dokazati tako što ćemo konstruirati jednu takvu iz proizvoljnog nepraznog skupa X. Neka je $X \neq \emptyset$, a X^{-1} takav da je $X \cap X^{-1} = \emptyset$ i postoji bijekcija $X \to X^{-1}$, koju označavamo s $x \to x^{-1}$.
Alfabet na skup X definiramo s $X \cup X^{-1}$. Za $n \in N$ definiramo riječ na X duljine $n \geqslant 1$ kao funkciju $\omega : \{1, ..., n\} \to X \cup X^{-1}$. Riječ ω zapisujemo na sljedeći način: ako je $\omega(i) = x_i^{e_i}$, onda je

$$\omega = x_1^{e_1}...x_n^{e_n}, \text{ gdje je } x_i \in X, \text{ a } e_i = \pm 1.$$

Duljinu riječi ω označavamo s $|\omega|$. Praznu riječ označavamo s 1. Duljina prazne riječi je 0. Svaka riječ ima jedinstven zapis, tj. ako su $u = x_1^{e_1}...x_n^{e_n}$ i $v = y_1^{d_1}...y_m^{d_m}$ riječi, gdje je $x_i, y_j \in X$, te $e_i = \pm 1$ i $d_j = \pm 1$, za svaki $i \leq n, j \leq m$, onda je $u = v$ ako i samo ako je $m = n, x_i = y_i$ i $e_i = f_i$.

Definicija 2.2.2. *Podriječ riječi $\omega = x_1^{e_1}...x_n^{e_n}$ je ili prazna riječ ili riječ oblika $u = x_r^{e_r}...x_s^{e_s}$, gdje je $1 \leq r \leq s \leq n$.*
Riječ ω je reducirana ako je $\omega = 1$ ili ω nema podriječi oblika xx^{-1} ili $x^{-1}x$, gdje je $x \in X$.

Definicija 2.2.3. *Inverz riječi $\omega = x_1^{e_1}...x_n^{e_n}$ je riječ $\omega^{-1} = x_n^{-e_n}...x_1^{-e_1}$.*

Definicija 2.2.4. *Neka su $u = x_1^{e_1}...x_n^{e_n}$ i $v = y_1^{d_1}...y_m^{d_m}$ riječi na X. Definiramo riječ*

$$uv = x_1^{e_1}...x_n^{e_n}y_1^{d_1}...y_m^{d_m}, \tag{2.1}$$

tj. riječ uv je nastala dopisivanjem riječi v do riječi u s desne strane.
Za $v = 1$ definiramo $u1 = 1u = u$.

Prva ideja je definirati slobodnu grupu F kao skup svih riječi na X s operacijom definiranom relacijom (2.1). Neutralni element bi bila prazna riječ 1, a inverz naravno inverzna riječ. Problem je što bi za neutralni element 1 trebalo vrijediti $xx^{-1} = 1$ za svaki $x \in X$. Međutim, to očito ne vrijedi jer je $|xx^{-1}| = 2$, dok je duljina prazne riječi jednaka 0. Taj problem možemo pokušati riješiti tako da za elemente slobodne grupe uzmemo samo reducirane riječi na X. Ali, čak i ako su u i v reducirane riječi, uv ne mora nužno biti reducirana riječ. Npr. neka su $u = xyz$ i $v = z^{-1}x$ riječi na X. Tada je $uv = xyzz^{-1}x$ i očito nije reducirana riječ. Rješavanje tog problem uzimanjem za binarnu operaciju operaciju definiranu relacijom (2.1) nakon koje je bi slijedilo reduciranje riječi dovodi do poteškoća u dokazivanju asocijativnosti.
Budući da želimo izjednačiti riječi oblika xx^{-1} i 1, te riječi oblika $xyzz^{-1}x$ i xyx, javlja se ideja definiranja neke relacije ekvivalencije na skupu svih riječi na X.

Definicija 2.2.5. *Neka su A i B riječi na X, mogu biti i prazne, te neka je $\omega = AB$. Elementarna operacija je ili umetanje, tj. pretvaranje riječi $\omega = AB$ u riječ oblika $\omega = Aaa^{-1}B$,* *gdje je $a \in X$, ili brisanje podriječi od ω oblika aa^{-1}, tj. pretvaranje riječi $\omega = Aaa^{-1}B$ u riječ AB.*

S $\omega \to \omega'$ označavamo da smo riječ ω' dobili iz riječi ω putem elementarnih operacija.

Definicija 2.2.6. *Dvije riječi u i v na X su ekvivalentne, u oznaci $u \sim v$, ako postoje riječi $u = \omega_1, \omega_2, ..., \omega_n = v$, te elementarne operacije*

$$u = \omega_1 \to \omega_2 \to ... \to \omega_n = v.$$

Klasu ekvivalencije riječi ω označavamo s $[\omega]$.
Primijetimo da je $xx^{-1} \sim 1$ i $x^{-1}x \sim 1$, tj. $[xx^{-1}] = [1] = [x^{-1}x]$

Ideja je definirati F kao skup svih klasa ekvivalencije. Najprije ćemo dokazati neka svojstva skupa svih riječi na X i definirane relacije ekvivalencije.

Definicija 2.2.7. *Neka je G neprazan skup i $\cdot$ binarna operacija na G. Kažemo da je $(G, \cdot)$ monoid ako vrijedi asocijativnost, te G sadrži neutralni element. Ako su skupovi S i S' monoidi, onda je preslikavanje $f : S \to S'$ homomorfizam ako zadovoljava:*

$$f(xy) = f(x)f(y) \text{ za svaki } x, y \in S \text{ i } f(e_S) = e_{S'}.$$

Lema 2.2.8. *Neka je X neki skup, a $W(X)$ skup svih riječi na X (ako je $X = \emptyset$, onda je $W(X) = \{1\}$). Tada vrijede sljedeće tvrdnje.*

(i) Skup $W(X)$ je uz operaciju definiranu relacijom (2.1) monoid.

(ii) Ako je $u \sim u'$ i $v \sim v'$, onda je $uv \sim u'v'$.

(iii) Ako je G grupa i $f : X \to G$ funkcija, tada postoji homomorfizam $\tilde{f} : W(X) \to G$ koji proširuje f, takav da iz $\omega \sim \omega'$ slijedi da je $\tilde{f}(\omega) = \tilde{f}(\omega')$ u G.

Dokaz. (i) Neka su $x = x_1^{e_1}...x_n^{e_n}$, $y = y_1^{d_1}...y_m^{d_m}$, te $z = z_1^{k_1}...z_r^{k_r}$ riječi na X. Tada je

$$\begin{aligned} (xy)z &= (x_1^{e_1}...x_n^{e_n}y_1^{d_1}...y_m^{d_m})z_1^{k_1}...z_r^{k_r} = \\ &= x_1^{e_1}...x_n^{e_n}y_1^{d_1}...y_m^{d_m}z_1^{k_1}...z_r^{k_r} = \\ &= x_1^{e_1}...x_n^{e_n}(y_1^{d_1}...y_m^{d_m}z_1^{k_1}...z_r^{k_r}) = \\ &= x(yz). \end{aligned}$$

Dakle, vrijedi $(xy)z = x(yz)$ za svaki $x, y, z \in W(X)$, tj. zadovoljen je zakon asocijativnosti. Skup $W(X)$ sadrži sve riječi na X, pa je i $1 \in W(X)$. Slijedi da je $W(X)$ monoid.

(ii) Neka su $u, v \in W(X)$. Kada elementarnu operaciju $u \to u'$ primjenimo na riječ uv dobijemo riječ $u'v$. Kada na riječ $u'v$ primjenimo elementarnu operaciju $v \to v'$ dobijemo $u'v'$. Dakle, imamo da je

$$uv \to u'v \to u'v'.$$

Slijedi da je $uv \sim u'v'$.

(iii) Neka je $\omega = x_1^{e_1}...x_n^{e_n}$ riječ na X. Definiramo $\tilde{f} : W(X) \to G$ s

$$\tilde{f}(\omega) = f(x_1)^{e_1}...f(x_n)^{e_n}. \tag{2.2}$$

Budući da ω ima jedinstven zapis, funkcija $\tilde{f}$ je dobro definirana.
Neka je $u = y_1^{d_1}...y_m^{d_m}$ riječ na X. Tada je

$$\tilde{f}(\omega u) = f(x_1)^{e_1}...f(x_n)^{e_n} f(y_1)^{d_1}...f(y_m)^{d_m} = \tilde{f}(\omega)\tilde{f}(u).$$

Dakle, $\tilde{f}$ je homomorfizam.
Neka je $\omega \sim \omega'$. Indukcijom po broju elementarnih operacija u lanci iz ω u ω' dokazujemo da je $\tilde{f}(\omega) = \tilde{f}(\omega')$.
Pretpostavimo da smo radili brisanje podriječi aa^{-1}, tj. promatramo

$$\omega = Aaa^{-1}B \to AB, \text{ gdje su } A, B \text{ podriječi od } \omega.$$

Tada imamo

$$\tilde{f}(Aaa^{-1}B) = \tilde{f}(A)\tilde{f}(a)\tilde{f}(a)^{-1}\tilde{f}(B) = \tilde{f}(A)\tilde{f}(B).$$

Na sličan način dokazujemo za slučaj kada radimo umetanje podriječi.

□

Propozicija 2.2.9. *Svaka riječ ω na skupu X je ekvivalentna jedinstvenoj reduciranoj riječi.*

Dokaz. Ako je $X = \emptyset$, onda postoji samo jedna riječ na X, prazna riječ 1, a 1 je reducirana riječ.
Neka je $X \neq \emptyset$. Najprije dokazujemo da postoji reducirana riječ ekvivalentna s ω. Ako ω nema podriječi oblika aa^{-1}, gdje je $a \in X \cup X^{-1}$, onda je ω reducirana riječ. Inače, brišemo prvu takvu podriječ. Tako dobivamo novu riječ ω_1, koja može biti i prazna, te za koju vrijedi $|\omega_1| < |\omega|$. Ako je ω_1 reducirana riječ gotovi smo. Inače, ponavljamo postupak i dobivamo novu kraću riječ ω_2. Budući da duljina riječi strogo opada, proces mora završiti s reduciranom riječi ekvivalentnom s ω (proces najdalje može ići do prazne riječi 1).
Da bismo dokazali jedinstvenost pretpostavimo suprotno, tj. da postoje dvije reducirane riječi u i v ekvivalentene s ω, te proces elementarnih operacija

$$u = \omega_1 \to \omega_2 \to ... \to \omega_n = v.$$

Možemo pretpostaviti da je n minimalan.
Budući da su u i v reducirane prva operacija je umetanje podriječi, dok je zadnja operacija brisanje podriječi. Neka je prvo brisanje dano s $\omega_i \to \omega_{i+1}$. Pretpostavimo da smo s elementarnom operacijom $\omega_{i-1} \to \omega_i$ umetnuli podriječ aa^{-1}, a zatim s $\omega_i \to \omega_{i+1}$ brisali podriječ bb^{-1}, gdje su $a, b \in X \cup X^{-1}$.
Postoje tri slučaja.

(i) Ako su podriječi aa^{-1} i bb^{-1} od ω_i jednake, onda je $\omega_{i-1} = \omega_{i+1}$ jer je ω_{i+1} dobivena iz ω_{i-1} umetanjem podriječi aa^{-1}, te zatim brisanjem iste. Dakle, imamo lanac

$$u = \omega_1 \to \omega_2 \to ... \to \omega_{i-1} = \omega_{i+1} \to ... \to \omega_n = v$$

koji je kraći od orginalnog najkraćeg lanaca.

(ii) Drugi slučaj je da se aa^{-1} i bb^{-1} preklapaju. To se može dogoditi na dva načina. Prvi je da je

$$\omega_i = Aaa^{-1}b^{-1}C,$$

gdje su A i C podriječi od ω_i, te $a^{-1} = b$, tj. $a = b^{-1}$. Dakle, $\omega_i = Aaa^{-1}aC$. Stoga je $\omega_{i-1} = AaC$ jer radimo umetanje aa^{-1}, te $\omega_{i+1} = AaC$ jer brišemo $bb^{-1} = a^{-1}a$. Dakle, $\omega_{i-1} = \omega_{i+1}$ i uklanjanjem ω_i dobivamo kraći lanac.
Drugi način preklapanja je

$$\omega_i = Aa^{-1}aa^{-1}C,$$

gdje je $b^{-1} = a$, što također vodi do $\omega_{i-1} = \omega_{i+1}$.

(iii) Treći slučaj je da se aa^{-1} i bb^{-1} ne preklapaju. Imamo da je

$$\omega_i = A'aa^{-1}A''bb^{-1}C \quad \text{i} \quad \omega_{i+1} = A'aa^{-1}A''C,$$

gdje je bb^{-1} postala podriječ od ω_i ranijim umetanjem ili bb^{-1} ili $b^{-1}b$ u $\omega_{j-1} = XY$, gdje je $j < i$. Na taj način smo dobili $\omega_j = Xbb^{-1}Y$ ili $\omega_j = Xb^{-1}bY$. U prvom slučaju podlanac $\omega_{j-1} \to ... \to \omega_{i+1}$ izgleda na sljedeći način

$$XY \to Xbb^{-1}Y \to ... \to Abb^{-1}C \to A'aa^{-1}A''bb^{-1}C \to A'aa^{-1}A''C,$$

gdje je $A = A'A''$. Ovaj lanac možemo skratiti tako što ne umetnemo bb^{-1} čime dobivamo

$$XY \to ... \to AC \to A'aa^{-1}A''C.$$

Jedini način na koji se, u slučaju da smo u riječ $\omega_{j-1} = XY$ umetnuli $b^{-1}b$, može dogoditi brisanje podriječi bb^{-1} je ako je $X = X'b$ ili $Y = b^{-1}Y'$. Ako je $X = X'b$, onda je $\omega_{j-1} = X'bY$, a $\omega_j = Xbb^{-1}bY$. Lanac

$$X'bY \to X'bb^{-1}bY \to ... \to Abb^{-1}C \to A'aa^{-1}A''bb^{-1}C \to A'aa^{-1}A''C,$$

gdje u procesima $X' \to A$ i $bY \to C$ imamo samo umetanje, možemo skratiti tako što ne umetnemo $b^{-1}b$ čime dobivamo lanac

$$X'bY \to ... \to AC \to A'aa^{-1}A''C.$$

Analogno radimo u slučaju kad je $Y = b^{-1}Y'$.

Budući da u svim slučajevima možemo skratiti lanac za koji smo pretpostavili da je najkraći, zaključujemo da takav lanac ne postoji. Dakle, ne postoje dvije različite reducirane riječi ekvivalentene s ω, tj. ω je ekvivalentna jedinstvenoj reduciranoj riječi. □

U sljedećem teoremu konačno konstruiramo slobodu grupu s bazom X.

Teorem 2.2.10. *Neka je X neki skup i F skup svih klasa ekvivalencije riječi na X. Tada je F uz operaciju $[u][v] = [uv]$ slobodna grupa s bazom $\{[x] : x \in X\}$.*
Štoviše, svaki element od F ima normalni oblik: za svaki $[u] \in F$ postoji jedinstvena reducirana riječ ω takav da je $[u] = [\omega]$.

Dokaz. Ako je $X = \emptyset$, onda $W(X)$ sadrži samo praznu riječ 1, pa je $F = \{1\}$.
Pretpostavimo sad da je $X \neq \emptyset$. U lemi 2.2.8 smo vidjeli da

$$u \sim u', v \sim v' \Rightarrow uv \sim u'v'.$$

Slijedi da je operacija $[u][v] = [uv]$ dobro definirana.
Prvo dokazujemo da je F grupa.
Asocijativnost: neka su $[u], [v], [w] \in F$. Budući da je asocijativnost zadovoljena u $W(X)$ vrijedi

$$[u]([v][w]) = [u][vw] = [u(vw)] = [(uv)w] = [uv][w] = ([u][v])[w].$$

Neutralni element: neutralni element je klasa $[1]$ jer za svaki $[u] \in F$ vrijedi

$$[u][1] = [u1] = [u]$$

$$[1][u] = [1u] = [u].$$

Inverzni element: inverzni element od $[u] \in F$ je $[u^{-1}] \in F$ jer je

$$[u][u^{-1}] = [uu^{-1}] = [1] = [u^{-1}u] = [u^{-1}][u].$$

Dakle, F je grupa.
Sada ćemo dokazati da je F slobodna grupa.
Ako je $[\omega] \in F$, onda je

$$[\omega] = [x_1^{e_1}...x_n^{e_n}] = [x_1^{e_1}]...[x_n^{e_n}],$$

gdje $e_i = \pm 1$ i $x_i \in X$, za svaki $i \leq n$. Dakle, ako svaki $x \in X$ identificiramo s $[x]$, grupa F je generirana s X.
U propoziciji 2.2.9 smo dokazali da za svaki $[\omega]$ postoji jedinstvena reducirana riječ u takva da je $[\omega] = [u]$. Da bismo dokazali da je F slobodna grupa s bazom X, neka je $f : X \to G$, gdje je G. Definiramo $\varphi : F \to G$ s

$$\varphi([x_1^{e_1}]...[x_n^{e_n}]) = f(x_1)^{e_1}...f(x_n)^{e_n},$$

gdje je $x_1^{e_1}...x_n^{e_n}$ reducirana riječ. Sada, iz jedinstvenosti reducirane riječi u svakoj klasi ekvivalencije slijedi da je funkcija φ dobro definirana. Očito φ proširuje f. Neka je

$$\tilde{f} : W(X) \to G$$

homomorfizam definiran u lemi 2.2.8 (formulom 2.2), a ω reducirana riječ. Tada je

$$\varphi([\omega]) = \tilde{f}(\omega).$$

Preostaje još dokazati da je φ homomorfizam. Neka su $[u], [v] \in F$, gdje su u i v reducirane riječi i neka je $uv \sim \omega$, gdje je ω reducirana riječ. Tada je

$$\varphi([u][v]) = \varphi([uv]) = \varphi([\omega]) = \tilde{f}(\omega)$$

jer je ω reducirana.
S druge strane je

$$\varphi([u])\varphi([v]) = \tilde{f}(u)\tilde{f}(v) = \tilde{f}(uv) = \tilde{f}(\omega)$$

jer su u, v reducirane i prema lemi 2.2.8

$$uv \sim \omega \Rightarrow \tilde{f}(uv) = \tilde{f}(\omega).$$

Slijedi da je

$$\varphi([u][v]) = \tilde{f}(\omega) = \varphi([u])\varphi([v]).$$

Dakle, φ je homomorfizam. Jedinstvenost homomorfizma φ slijedi iz činjenice da X generira F. □

Budući da je svaka riječ na X ekvivalentna jedinstvenoj reduciranoj riječi, reducirane riječi možemo uzeti za predstavnike klasa ekvivalencije. Stoga slobodnu grupu F možemo promatrati kao skup svih reduciranih riječi na X uz operaciju definiranu relacijom (2.1) nakon koje slijedi redukcija.
Kao i kod običnih grupa, i slobodne grupe želimo međusobno usporediti.

Propozicija 2.2.11. *(i) Neka je X_1 baza slobodne grupe F_1, a X_2 baza slobodne grupe F_2. Ako je $f : X_1 \to X_2$ bijekcija, onda postoji izomorfizam $\varphi : F_1 \to F_2$ koji proširuje f.*

(ii) Ako je F slobodna grupa s bazom X, onda je F generirana s X.

Dokaz. (i) Budući da je $X_2 \subseteq F_2$ možemo uzeti da je $f : X_1 \to F_2$. Grupa je F_1 slobodna grupa s bazom X_1, pa postoji jedinstven homomorfizam $\varphi_1 : F_1 \to F_2$ koji proširuje f.
Kako je f bijekcija, postoji inverzna funkcija $f^{-1} : X_2 \to X_1$. Ponovno, zbog $X_1 \subseteq F_1$, možemo uzeti da je $f^{-1} : X_2 \to F_1$. S obzirom da je F_2 slobodna grupa s bazom X_2, postoji jedinstven homomorfizam $\varphi_2 : F_2 \to F_1$ koji proširuje f^{-1}.
Slijedi da je $\varphi_2\varphi_1 : F_1 \to F_2$ homomorfizam koji proširuje 1_{X_1}. Međutim, identiteta 1_{F_1} je također homomorfizam koji proširuje 1_{X_1}, pa iz jedinstvenosti proširenja slijedi da je $\varphi_2\varphi_1 = 1_{X_1}$. Analogno se dokazuje da je $\varphi_1\varphi_2 = 1_{X_2}$. Slijedi da je homomorfizam φ_1 bijekcija, tj. φ_1 je izomorfizam.

(ii) Neka je $f : X_1 \to X$ bijekcija, a F_1 slobodna grupa s bazom X_1 konstruirana kao u teoremu 2.2.10. Slijedi da je F_1 generirana s X_1. Prema (i) postoji izomorfizam $\varphi : F_1 \to F$ takav da je $\varphi(X_1) = X$. Budući da X_1 generira F_1, slijedi da $\varphi(X_1)$ generira $\operatorname{Im}\varphi$, tj. X generira F.

□

Kao i za slobodne Abelove grupe, i ovdje želimo definirati rang.

Lema 2.2.12. *Ako je F slobodna grupa s bazom $X = \{x_1, ..., x_n\}$, onda je F/F' slobodna Abelova grupa s bazom $X' = \{x_1F', ..., x_nF'\}$, gdje je F' komutatorska podgrupa grupe F.*

Dokaz. Prema prethodnoj propoziciji, X generira F. Stoga X' generira F/F'. Po kriteriju propozicije 2.1.11 dokazujemo da je F/F' slobodna Abelova grupa s bazom X'.
Neka su
$$p : X \to F \quad \text{i} \quad p' : X' \to F/F'$$
inkluzije, $\pi : F \to F/F'$ prirodno preslikavanje,
$$\nu : X \to X' \quad \text{definirana s} \quad \nu(x) = xF',$$
te $\gamma : X' \to G$, gdje je G Abelova grupa. Prema definiciji slobodne grupe, postoji jedinstven homomorfizam
$$g : F \to G \quad \text{sa svojstvom} \quad gp = \gamma\nu,$$
tj. g je proširenje funkcije $\gamma\nu : X \to G$.
Definiramo
$$g' : F/F' \to G \quad \text{s} \quad g'(wF') = g(w).$$
Preslikavanje g' je dobro definirano jer je G Abelova, pa slijedi da je $F' \leq \operatorname{Ker} g$. Imamo da je
$$g'p'\nu = g'\pi p = gp = \gamma\nu.$$

Budući da je ν surjekcija, slijedi da je $g'p' = \gamma$. Konačno, g' je jedinstveno takvo preslikavanje, jer ako preslikavanje g'' zadovoljava $g''p' = \gamma$, onda su preslikavanja g' i g'' jednaka na generirajućem skupu X. Slijedi da su jednaka na F/F'. □

Propozicija 2.2.13. *Neka je F slobodna grupa s bazom X. Ako je $|X| = n$, onda svaka baza od F ima n elemenata.*

Dokaz. Prema lemi 2.2.12, F/F' je slobodna Abelova grupa ranga n. Ako je s druge strane $\{y_1, ..., y_m\}$ neka druga baza od F, onda je F/F' slobodna Abelova grupa ranga m. Prema propoziciji 2.1.8 slijedi da je $m = n$. □

Sada možemo definirati rang.

Definicija 2.2.14. *Rang slobodne grupe F, u oznaci $rang(F)$, je broj elemenata baze od F.*

Propoziciju 2.2.11 (i) sada možemo izraziti na sljedeći način: dvije slobodne grupe su izomorfne ako i samo ako im je jednak rang.
Sljedeća propozicija nam daje vezu između slobodnih grupa i grupa općenito.

Propozicija 2.2.15. *Svaka grupa G je kvocijent slobodne grupe.*

Dokaz. Neka je X skup za koji postoji bijekcija $f : X \to G$ (npr. $f = 1_G : G \to G$) i neka je F slobodna grupa s bazom X. Prema definiciji slobodne grupe postoji homomorfizam $\varphi : F \to G$ koji proširuje f. Preslikavanje φ je surjekcija jer je f surjekcija. Prema *Prvom teoremu o izomorfizmu* slijedi da je $G \cong F/\operatorname{Ker} f$. □

Definicija 2.2.16. *Prezentacija grupe G je uređeni par*

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

gdje je X skup, R skup riječi na X, te $G = F/N$, gdje je F slobodna grupa s bazom X, a N normalna podgrupa generirana s R, tj. podgrupa generirana sa svim konjugatima elemenata iz R. Skup X zovemo generatorima, a skup R relacijama.

Propozicija 2.2.15 nam govori da svaka grupa ima prezentaciju.
Slobodna grupa s bazom X ima prezentaciju

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

Dakle, u prezentaciji slobodne grupe nema relacija. Odatle potječe i naziv slobodne grupe, tj. riječ je o grupi „slobodnoj od relacija ”.

Lema 2.2.17. *Neka je F slobodna grupa s bazom X i neka je $A \subseteq X$. Ako je N normalna podgrupa generirana s A, onda je F/N slobodna grupa.*

Dokaz. Tvrdimo da je F/N slobodna grupa s bazom $B = \{xN : x \in X \setminus A\}$. Očito B generira F/N. Neka je G grupa i $f : B \to G$ neka funkcija. Definiramo $g : X \to G$ s

$$g(x) = \begin{cases} f(xN), & x \in X \setminus A, \\ e_G, & x \in A. \end{cases}$$

Budući da je F slobodna grupa s bazom X, postoji jedinstven homomorfizam $\varphi : F \to G$ koji proširuje funkciju g.
Skup A generira N, pa slijedi da je $N \subseteq \operatorname{Ker} \varphi$. Stoga je preslikavanje $\tilde{\varphi} : F/N \to G$ definirano s

$$\tilde{\varphi}(yN) = \varphi(y) \quad za\ y \in F$$

homomorfizam. Pokažimo da $\tilde{\varphi}$ proširuje f. Ako je $xN \in B$, za $x \in X \setminus A$, onda je

$$\tilde{\varphi}(xN) = \varphi(x) = g(x) = f(xN).$$

Jedinstvenost homomorfizama $\tilde{\varphi}$ slijedi iz činjenice da B generira F/N. □

2.3 Nielsen-Schreierov teorem

Nakon što smo definirali slobodne grupe i naveli neka njihova osnovna svojstva, u ovom potpoglavlju ćemo dokazati jedan od fundamentalnih teorema o slobodnim grupa, što je i cilj ovog rada. To je Nielsen-Schreierov teorem koji kaže da je svaka podgrupa slobodne grupe također slobodna grupa. Za dokaz teorema je potrebno još definirati poseban podskup grupe koji nazivamo transverzala.

Definicija 2.3.1. *Neka je S podgrupa grupe G. Transverzala ℓ od S u G je podskup od G koji sadrži točno jedan element $\ell(Sb) \in Sb$, za svaku klasu Sb, te vrijedi $\ell(S) = 1$.*

Neka je F slobodna grupa s bazom X, a $S \leq F$. Ako je dana transverzala ℓ od S u F, onda za svaki $x \in X$ vrijedi da $\ell(Sb)x, \ell(Sbx) \in Sbx$. Stoga je

$$t_{Sb,x} = \ell(Sb)x\ell(Sbx)^{-1} \in S. \tag{2.3}$$

Sada definiramo slobodnu grupu Y čiji bazu čine $y_{Sb,x}$, takvi da je preslikavanje definirano s $y_{Sb,x} \to t_{Sb,x}$ bijekcija. Definiramo homomorfizam

$$\varphi : Y \to S \quad \text{s} \quad y_{Sb,x} \to t_{Sb,x}.$$

Zatim, za svaku klasu Sb definiramo funkciju

$$F \to Y \quad \text{koju označavamo s} \quad u \to u^{Sb}.$$

Ove funkcije definiramo induktivno po $|u| \geq 0$, gdje je u reducirana riječ na X. Za svaki $x \in X$ i za svaku lijevu klasu Sb definiramo

$$1^{Sb} = 1, \quad x^{Sb} = y_{Sb,x}, \quad (x^{-1})^{Sb} = (x^{Sbx^{-1}})^{-1}. \tag{2.4}$$

Ako je $u = x^{\varepsilon}v$ reducirana riječ duljine $n+1$, gdje je $\varepsilon = \pm 1$, a $|v| = n$, definiramo

$$u^{Sb} = (x^{\varepsilon})^{Sb} v^{Sbx^{\varepsilon}}.$$

Navedimo sada neka svojstva ovih funkcija.

Lema 2.3.2. *(i) Za svaki $u, v \in F$ vrijedi $(uv)^{Sb} = u^{Sb}v^{Sbu}$.*

(ii) Za svaki $u \in F$ je $(u^{-1})^{Sb} = (u^{Sbu^{-1}})^{-1}$.

(iii) Ako je $\varphi : Y \to S$ homomorfizam definiran s

$$\varphi : y_{Sb,x} \to t_{Sb,x} = \ell(Sb)x\ell(Sbx)^{-1},$$

onda je za svaki $u \in F$, $\varphi(u^{Sb}) = \ell(Sb)u\ell(Sbu)^{-1}$.

(iv) Funkcija $\theta : S \to Y$, definirana s $\theta : u \to u^S$ je homomorfizam, te vrijedi $\varphi\theta = 1_S$.

Dokaz. (i) Dokazujemo indukcijom po $|u|$, gdje je u reducirana riječ. Ako je $|u| = 0$, onda je $u = 1$, te vrijedi $(uv)^{Sb} = v^{Sb}$. S druge strane je $1^{Sb}v^{Sb1} = v^{Sb}$. Dakle, $(uv)^{Sb} = u^{Sb}v^{Sbu}$.

Za korak indukcije neka je $u = x^{\varepsilon}w$. Tada je

$$\begin{aligned}(uv)^{Sb} &= (x^{\varepsilon})^{Sb}(wv)^{Sbx^{\varepsilon}} = (x^{\varepsilon})^{Sb}w^{Sbx^{\varepsilon}}v^{Sbx^{\varepsilon}w} \\ &= (x^{\varepsilon})^{Sb}w^{Sbx^{\varepsilon}}v^{Sbu} = (x^{\varepsilon}w)^{Sb}v^{Sbu} = u^{Sb}v^{Sbu}.\end{aligned}$$

(ii) Tvrdnja slijedi iz

$$1 = 1^{Sb} = (u^{-1}u)^{Sb} = (u^{-1})^{Sb}u^{Sbu^{-1}}.$$

(iii) Primijetimo da je φ homomorfizam jer je Y slobodna grupa čije bazu čine svi $y_{Sb,x}$. Ponovno dokazujemo indukcijom po $|u| \geq 0$.

Za praznu riječ je

$$\varphi(1^{Sb}) = \varphi(1) = 1 = \ell(S)1\ell(S1)^{-1}.$$

Za korak indukcije, neka je $u = x^{\varepsilon}v$, gdje je u reducirana riječ. Tada je

$$\begin{aligned}\varphi(u^{Sb}) &= \varphi((x^{\varepsilon}v)^{Sb}) = \varphi((x^{\varepsilon})^{Sb}v^{Sbx^{\varepsilon}}) = \varphi((x^{\varepsilon})^{Sb})\varphi(v^{Sbx^{\varepsilon}}) \\ &= \varphi((x^{\varepsilon})^{Sb})\ell(Sbx^{\varepsilon})v\ell(Sbx^{\varepsilon}v)^{-1}.\end{aligned}$$

Postoje dva slučaja ovisno o predznaku ε. Ako je $\varepsilon = 1$, onda je

$$\varphi(u^{Sb}) = \ell(Sb)x\ell(Sbx)^{-1}\ell(Sbx)v\ell(Sbxv)^{-1} = \ell(Sb)xv\ell(Sbu)^{-1} = \ell(Sb)u\ell(Sbu)^{-1}.$$

Ako je $\varepsilon = -1$, onda je

$$\begin{aligned}\varphi(u^{Sb}) &= \varphi((y_{Sbx^{-1},x})^{-1})\ell(Sbx^{-1})v\ell(Sbx^{-1}v)^{-1}\\ &= (\ell(Sbx^{-1})x\ell(Sbx^{-1}x)^{-1})^{-1}\ell(Sbx^{-1})v\ell(Sbx^{-1}v)^{-1}\\ &= \ell(Sb)x^{-1}\ell(Sbx^{-1})^{-1}\ell(Sbx^{-1})v\ell(Sbx^{-1}v)^{-1}\\ &= \ell(Sb)x^{-1}v\ell(Sbx^{-1}v)^{-1} = \ell(Sb)u\ell(Sbu)^{-1}.\end{aligned}$$

(iv) Za $u \in S$, definiramo $\theta : S \to Y$ s

$$\theta : u \to u^S.$$

Sada, ako je $u, v \in S$, onda je

$$\theta(uv) = (uv)^S = u^S v^{Su} = u^S v^S = \theta(u)\theta(v),$$

jer za $u \in S$ imamo da je $Su = S$. Stoga je θ homomorfizam. Štoviše, ako je $u \in S$, onda iz (iii) slijedi da je

$$\varphi\theta(u) = \varphi(u^S) = \ell(S1)u\ell(S1u) = u.$$

□

Korolar 2.3.3. *Ako je S podgrupa slobodne grupe F, te ℓ transverzala od S u F, onda skup svih $t_{Sb,x}$ različitih od 1 generira S.*

Dokaz. Budući da je $\varphi\theta = 1_S$, funkcija $\varphi : Y \to S$ je surjekcija. Slijedi da slike $t_{Sb,x}$ generatora $y_{Sb,x}$ od Y generiraju $\operatorname{Im}\varphi = S$. Naravno, ako se u skupu generatora pojavi prazna riječ 1, možemo je izbaciti. □

Lema 2.3.4. *Ako je ℓ transverzala od S u F, onda je* $\operatorname{Ker}\varphi$ *normalna podgrupa grupe Y generirana sa svim $\ell(Sb)^S$.*

Dokaz. Neka je N normalna podgrupa od Y generirana sa svim $\ell(Sb)^S$, a $K = \operatorname{Ker}\varphi$. Neka je $\theta : S \to Y$ definirana s $u \to u^S$. Prema lemi 2.3.2 (iv) je θ homomorfizam takav da je $\varphi\theta = 1_S$. Stoga je prema lemi 2.2.17 K normalna podgrupa generirana s $\{y^{-1}\rho(y) : y \in Y\}$, gdje je $\rho = \theta\varphi$.
Prema lemi 2.3.2 (i) je

$$\begin{aligned}y_{Sb,x}^{-1}\rho(y_{Sb,x}) &= y_{Sb,x}^{-1}(\ell(Sb)x\ell(Sbx)^{-1})^S\\ &= y_{Sb,x}^{-1}\ell(Sb)^S x^{Sb}(\ell(Sbx)^{-1})^{Sbx}\\ &= (y_{Sb,x}^{-1}\ell(Sb)^S y_{Sb,x})(\ell(Sbx)^{-1})^{Sbx},\end{aligned}$$

jer prema definiciji funkcije $u \to u^{Sb}$ (formulom 2.4) vrijedi $x^{Sb} = y_{Sb,x}$. Stoga je

$$y_{Sb,x}^{-1}\rho(y_{Sb,x}) = (y_{Sb,x}^{-1}\ell(Sb)^S y_{Sb,x})(\ell(Sbx)^S)^{-1}. \tag{2.5}$$

Naime, prema lemi 2.3.2 (ii) je $(\ell(Sbx)^{-1})^{Sbx} = (\ell(Sbx)^S)^{-1}$. Iz jednadžbe (2.5) slijedi da $y_{Sb,x}^{-1}\rho(y_{Sb,x}) \in N$, pa je $K \leq N$.
Za obratnu inkluziju, prema jednadžbi (2.5) je $\ell(Sb)^S \in K$ ako i samo ako je $\ell(Sbx)^S \in K$. Stoga se potrebana inkluzija može dokazati indukcijom po $|\ell(Sb)|$, pa je $K = N$. □

Sada ćemo definirati posebanu transverzalu: Schreierovu transverzalu. Naime, ona nam je ključna za dokaz našeg teorema, jer će nam bazu podgrupe činiti $t_{Sb,x}$ definirani u jednadžbi (2.3) uz Schreierovu transverzalu.

Definicija 2.3.5. *Neka je F slobodna grupa s bazom X, te S podgrupa od F. Schreierova transverzala je transverzala ℓ sa svojstvom da, ako je $\ell(Sb) = x_1^{\varepsilon_1}x_2^{\varepsilon_2}...x_n^{\varepsilon_n}$ reducirana riječ, onda je svaki početni segment $x_1^{\varepsilon_1}...x_k^{\varepsilon_k}$, za $1 \leq k \leq n$, također element transverzale.*

Lema 2.3.6. *Schreierova transverzala postoji za svaku podgrupu S slobodne grupe F.*

Dokaz. Definiramo duljinu klase Sb, uz oznaku $|Sb|$, kao minimalnu duljinu elemenata $sb \in Sb$. Indukcijom po $|Sb|$ dokazujemo da postoji predstavnik $\ell(Sb) \in Sb$ takav da je svaki njegov početni segment predstavnik klase kraće duljine.
Počinjemo definiranjem $\ell(S) = 1$. Za korak indukcije neka je $|Sz| = n + 1$ i $ux^{\varepsilon} \in Sz$, gdje je $\varepsilon = \pm 1$, a $|ux^{\varepsilon}| = n + 1$. Slijedi da je $|Su| = n$. Naime, ako bi bilo $|Su| = m < n$, postojao bi predstavnik v duljine m. Tada bi vx^{ε} bio predstavnik od Sz duljine manje od $n+1$. Prema indukciji, postoji $b = \ell(Su)$ takav da je svaki njegov početni segment također predstavnik. Definiramo $\ell(Sz) = bx^{\varepsilon}$. □

Teorem 2.3.7. *(Nielsen-Schreierov teorem)*
Svaka podgrupa S slobodne grupe F je slobodna grupa. Preciznije, ako je X baza od F, a ℓ Schreierova transverzala od S u F, onda bazu od S čine svi $t_{Sb,x} = \ell(Sb)x\ell(Sbx)^{-1}$ različiti od 1.

Dokaz. Neka je $\theta : S \to Y$ definirano kao u lemi 2.3.2 (iv). Tada je je $\varphi\theta = 1_S$, pa je φ surjekcija, tj. $\operatorname{Im}\varphi = S$. Stoga je prema *Prvom teoremu o izomorfizmu* $S \cong Y/K$, gdje je $K = \operatorname{Ker}\varphi$. Prema lemi 2.3.4, K je normalna podgrupa od Y generirana sa svim $\ell(Sb)^S$, te je prema lemi 2.2.17 dovoljno dokazati da je K jednaka normalnoj podgrupi T generiranoj sa **specijalnim** $y_{Sb,x}$, tj. onima za koje je $\varphi(y_{Sb,x}) = t_{Sb,x} = 1$. Očito je $T \leq K$, pa je dovoljno dokazati obratnu inkluziju.
Indukcijom po $|\ell(Sv)|$ dokazujemo da je $\ell(Sv)^S$ riječ na specijalnim $y_{Sb,x}$.
Za $|\ell(Sv)| = 0$ je

$$\ell(Sv) = \ell(S) = 1,$$

što je riječ na specijalnim $y_{Sb,x}$.
Ako je $|\ell(Sv)| > 0$, onda je

$$\ell(Sv) = ux^{\varepsilon}, \text{ gdje je } \varepsilon = \pm 1, \text{ a } |u| < \ell(Sv).$$

Budući da je ℓ Schreierova transverzala, slijedi da je u također element transverzale: $u = \ell(Su)$. Prema Lemi 2.3.2 (i) je

$$\ell(Sv)^S = u^S (x^{\varepsilon})^{Su}.$$

Po pretpostavci indukcije, u^S je riječ na specijalnim $y_{Sb,x}$, pa je stoga $u^S \in T$.
Preostaje dokazati da je $(x^{\varepsilon})^{Su}$ riječ na specijalnim $y_{Sb,x}$.
Ako je $\varepsilon = 1$, onda je $(x^{\varepsilon})^{Su} = x^{Su} = y_{Su,x}$. Budući da je $\ell(Sux) = ux$, jer je $v = ux$, a ℓ Schreierova transverzala, imamo

$$\varphi(y_{Su,x}) = t_{Su,x} = \ell(Su)x\ell(Sux)^{-1} = ux(ux)^{-1} = 1.$$

Slijedi da je $x^{Su} \in T$.
Ako je $\varepsilon = -1$, onda imamo

$$(x^{-1})^{Su} = (x^{Sux^{-1}})^{-1} = (y_{Sux^{-1},x})^{-1}.$$

Dakle,

$$\varphi((x^{-1})^{Su}) = (t_{Sux^{-1},x})^{-1} = [(\ell(Sux^{-1})x\ell(Sux^{-1}x)]^{-1} = [\ell(Sux^{-1})x\ell(Su)]^{-1}.$$

Budući da je ℓ Schreierova transverzala, imamo da je

$$\ell(Su) = u \quad \text{i} \quad \ell(Sux^{-1}) = \ell(Sv) = v = ux^{-1}.$$

Dakle,

$$\varphi((x^{-1})^{Su}) = [(ux^{-1})xu^{-1}]^{-1} = 1.$$

Slijedi da je $(x^{-1})^{Su} \in T$, pa je $\ell(Sv)^S \in T$. Dakle, $T = K$. □

Slijedi nekoliko posljedica prethodnog teorema. Sljedeći korolar pokazuje da podgrupa konačnogenerirane grupe nije nužno konačnogenerirana.

Korolar 2.3.8. *Ako je F slobodna grupa ranga 2, onda je komutatorska podgrupa F' grupe F slobodna grupa beskonačnog ranga.*

Dokaz. Neka je $\{x, y\}$ baza grupe F. Budući da je prema lemi 2.2.12 F/F' slobodna Abelova grupa s bazom $\{xF', yF'\}$, svaka klasa $F'b$ ima jedinstvenog predstavnika oblika $x^m y^n$, gdje je $m, n \in \mathbb{Z}$. Slijedi da je transverzala definirana s $\ell(F'b)$ Schreierova transverzala jer je svaka podriječ riječi $x^m y^n$ jednakog oblika.
Ako je $n > 0$, onda je $\ell(F'y^n) = y^n$, dok je $\ell(F'y^n x) = xy^n \neq y^n x$. Stoga postoji beskonačno mnogo elemenata $t_{Sy^n,x} = \ell(F'y^n)x\ell(F'y^n x)^{-1} \neq 1$, pa tvrdnja slijedi prema Nielsen-Schreierovom teoremu. □

Iako proizvoljna podgrupa konačnogenerirane grupe nije nužno konačnogenerirana, sljedeći korolar pokazuje da podgrupa konačnog indeksa mora biti konačnogenerirana.

Korolar 2.3.9. *Ako je F slobodna grupa konačnog ranga n, tada je svaka podgrupa S grupe F konačnog indeksa j također konačnogenerirana. Preciznije, $rang(S) = jn - j + 1$.*

Dokaz. Neka je $X = \{x_1, ..., x_n\}$ baza od F, a $\ell = \{\ell(Sb)\}$ Schreierova transverzala. Prema Nielsen-Schreierovom teoremu, S je slobodna grupa čiju bazu čine $t_{Sb}, x \neq 1$, gdje je $x \in X$. Budući da postoji j izbora za Sb i n izbora za x, slijedi da baza od S može imati najviše jn elemenata. Dakle, $rang(S) \leq jn$, pa je S konačnogenerirana.
Za uređeni par (Sb, x) kažemo da je trivijalan ako je $t_{Sb,x} = 1$, tj. ako je $\ell(Sb)x = \ell(Sbx)$. Pokazat ćemo da postoji bijekcija ψ između familije klasa $\{Sb \neq S\}$ i trivijalnih uređenih parova, tako da postoji $j-1$ trivijalnih uređenih parova odakle će slijediti da je

$$rang(S) = jn - (j - 1) = jn - j + 1.$$

Za $Sb \neq S$ imamo da je $\ell(Sb) = b = ux^{\varepsilon}$. Budući da je ℓ Schreierova transverzala, slijedi da je $u \in \ell$. Definiramo $\psi(Sb)$ na sljedeći način

$$\psi(Sux^{\varepsilon}) = \begin{cases} (Su, x), & \varepsilon = 1, \\ (Sux^{-1}, x), & \varepsilon = -1. \end{cases}$$

Primijetimo da je $\psi(Sux^{\varepsilon})$ trivijalan uređeni par. Ako je $\varepsilon = 1$, onda je

$$\ell(Sux) = \ell(Sb) = b = ux.$$

Stoga je $\ell(Su)x = ux$ i $t_{Su,x} = 1$.
Ako je $\varepsilon = -1$, onda je

$$\ell(Sbx) = \ell(Sux^{-1}x) = \ell(Su) = u,$$

pa je $\ell(Sb)x = bx = ux^{-1}x = u$ i $t_{Sb,x} = 1$.
Da bismo vidjeli da je ψ injekcija, pretpostavimo da je

$$\psi(Sb) = \psi(Sc), \quad \text{gdje je} \quad b = ux^{\varepsilon},\ c = vy^{\eta}, \quad \text{za } x, y \in X, \text{ te } \varepsilon = \pm 1,\ \eta = \pm 1.$$

Postoje četiri mogućnosti ovisno o predznacima ε i η. To su

$$(Su, x) = (Sv, y), \quad (Su, x) = (Svy^{-1}, y),$$

$$(Sux^{-1}, x) = (Sv, y), \quad (Sux^{-1}, x) = (Svy^{-1}, y).$$

U svakom slučaju iz jednakosti uređenih parova slijedi $x = y$.
Ako je $(Su, x) = (Sv, x)$, onda je $Su = Sv$. Slijedi da je

$$Sb = Sux = Svx = Sc.$$

Ako je $(Su, x) = (Svx^{-1}, x)$, onda je $Su = Svx^{-1} = Sc$. Stoga je $\ell(Su) = \ell(Sc) = c$. Budući da je (Su, x) trivijalan uređen par vrijedi $\ell(Su)x = \ell(Sux) = b$. Slijedi da je

$$b = \ell(Su)x = cx = vx^{-1}x,$$

što je kontradikcija s činjenicom da je b reducirana riječ. Na sličan način se pokaže da ne može vrijediti $(Sux^{-1}, x) = (Sv, x)$.
Konačno, ako je $(Sux^{-1}, x) = (Svx^{-1}, x)$, onda je

$$Sb = Sux^{-1} = Svx^{-1} = Sc.$$

Pokažimo da je ψ surjekcija. Neka je (Sw, x) trivijalan uređen par, tj. takav da je

$$\ell(Sw)x = wx = \ell(Sw).$$

Imamo da je $w = ux^{\varepsilon}$, gdje je $u \in \ell$ i $\varepsilon = \pm 1$.
Ako je $\varepsilon = 1$, onda je $\psi(Swx) = (Sw, x)$, a ako je $\varepsilon = -1$, onda je

$$\psi(Su) = (Sux^{-1}, x) = (Sw, x).$$

□

Korolar 2.3.10. *Postoje neizomorfne konačnogenerirane grupe G i H, takve da postoji podgrupa grupe G izomorfna s H i postoji podgrupa grupe H izomorfna s G.*

Dokaz. Ako je G slobodna grupa ranga 2, a H slobodna grupa ranga 3, onda je $G \not\cong H$. Očito je G izomorfna podgrupi grupe H (prema propoziciji 2.2.11 (i) dvije slobodne grupe su izomorfne ako imaju jednak rang). S druge strane komutatorska pogrupa G' grupe G je beskonačnog ranga. Dakle, G' ima slobodnu podgrupu ranga 3. Stoga i G ima podgrupu ranga 3 i ta podgrupa je izomorfna grupi H. □

Bibliografija

[1] S. Lang, *Algebra*, second edition, Addison-Wesley Publishing Company, Reading, MA, 1984.
[2] J. J. Rotman, *Advanced Modern Algebra*, Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2010.
[3] B. Širola, *Algebarske strukture*, skripta, dostupno na http://web.math.pmf.unizg.hr/nastava/alg/predavanja/ (kolovoz 2014.).

Sažetak

U ovom radu dokazujemo jedan od fundamentalnih rezultata o slobodnim grupama. To je Nielsen-Schreierov teorem, koji kaže da je svaka podgrupa slobodne grupe također slobodna grupa.
Najprije ćemo definirati grupu, podgrupu, generiranu podgrupu, normalnu grupu, te kvocijentne grupe koje nam govore kako iz već postojeće grupe konstruirati novu grupu. Također ćemo definirati homomorfizam između grupa, i posebno izomorfizam, koji nam omogućuju da usporedimo grupe, te dokazati tri teorema o izomorfizmima.
U drugom ćemo dijelu najprije definirati direktnu sumu Abelovih grupa preko koje ćemo definirati slobodnu Abelovu grupu i njenu bazu. Karakterizacija slobodnih Abelovih grupa nam je motivacija za općenitu definiciju slobodnih grupa. Postojanje ne-abelove slobodne grupe dokazat ćemo tako što ćemo je konstruirati iz proizvoljnog nepraznog skupa, koji će biti baza za tu slobodnu grupu. Zatim ćemo definirati transverzalu i posebno Schreierovu transverzalu preko koje definiramo bazu za podgrupu slobodne grupe. Na kraju ćemo navesti nekoliko posljedica Nielsen-Schreierog teorema.

Summary

In this thesis we prove one of the fundamental results about free groups. That is the Nielsen-Schreier theorem, which says that every subgroup of free group is also free group. First, we define a group, a subgroup, a generated subgroup, a normal subgroup and quotient groups which allows us to construct a new group from given group. We will also define a homomorphism between groups, and specially an isomorphism, and prove the three isomorphism theorems.
In second part, first, we define a direct sum, which allows us to define a free abelian group and its basis. The characterisation of free abelian groups is our motivation for more general definition of free groups. We prove existence of non-abelian free group by constructing it from some nonempty set, which is a basis for that free group. Than, we define a transversal, and specially Schreier transversal, which allows us to define a basis for a subgroup of free group. In the end, we give some applications of the Nielsen-Schreier theorem.

Životopis

Rođena sam 6. siječnja 1989. godine u Livnu. U Livnu sam 1995. upisala sam Osnovnu školu Ivan Goran Kovačić. Nakon završetka osnovne škole 2003. upisujem se u Opću gimnaziju Livno. Maturirala sam 2007. s odličnim uspjehom te upisala Preddiplomski studij matematike na PMF-MO u Zagrebu. Po završetku prediplomskog studija upisala sam diplomski studij Financijska i poslovna matematika.