SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Marin Gunja

ZORNOVA LEMA I SRODNE TVRDNJE

Diplomski rad

Voditelj rada:
doc. dr. sc. Vedran Čačić

Zagreb, srpanj 2020.

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. ____________________________

Obitelji, prijateljima, kolegama, i svima ostalima koji su me nebrojeno puta pitali hoću li stići dovršiti ovaj rad.

Sadržaj

Uvod

U centru pažnje ovog rada je *Zornova lema*.

Teorem 0.0.1 (Zornova lema)**.** *Neka je* $(A, <)$ *parcijalno uređen skup koji ima svojstvo da svaki lanac u* A *ima gornju među u* A. *Tada* $(A, <)$ *ima barem jedan maksimalni element.*

Posebno je zanimljiva jer se koristi vjerojatno u svakoj grani matematike. Neki primjeri su navedeni na stranici 4. Također, u Zermelo–Fraenkelovoj teoriji skupova (ZF) ekvivalentna je *aksiomu izbora*. Jedan oblik u kojem se iskazuje je:

Aksiom 0.0.2 (Aksiom izbora)**.** Neka je X skup nepraznih u parovima disjunktnih skupova. Tada postoji skup B (*izborni skup*) takav da je $B \cap Y$ jednočlan skup za svaki $Y \in X$.

Da su tvrdnje ekvivalentne u ZF znači da se ekvivalencija može dokazati korištenjem aksioma ZF. Teorijom ZF se nećemo detaljnije baviti, ali se svi potrebni detalji, kao i njeni aksiomi, mogu pronaći u [3].

Možda se pitate zašto smo se odlučili pažnju obratiti na Zornovu lemu, a ne na aksiom izbora. Zornova lema predstavlja svojevrsno „sučelje” aksioma izbora — naime, aksiom izbora se, u svom „najčišćem” obliku, mnogo rjeđe primjenjuje nego Zornova lema.

U ovom radu ćemo navesti i određene kritike Zornove leme i (posljedično) aksioma izbora. Najčešća kritika na koju možemo naići je *nekonstruktivnost*. Naime, Zornovom lemom se dokazuje *postojanje* nekog maksimalnog elementa, ali najčešće nijedan maksimalni element ne možemo konstruirati. Primjeri će biti dani u radu.

Poglavlje 1

Aksiom izbora

1.1 Uvodno o aksiomu izbora

Aksiom izbora ima mnogo ekvivalentnih formulacija. Odlučili smo krenuti od formulacije za koju smatramo da je čitatelju intuitivno jasna bez detaljnijeg obrazloženja. Ponovimo je:

Aksiom 0.0.2. Neka je X skup nepraznih u parovima disjunktnih skupova. Tada postoji skup B (*izborni skup*) takav da je $B \cap Y$ jednočlan skup za svaki $Y \in X$.

Vizualni prikaz aksioma izbora je na Slici 1.1.

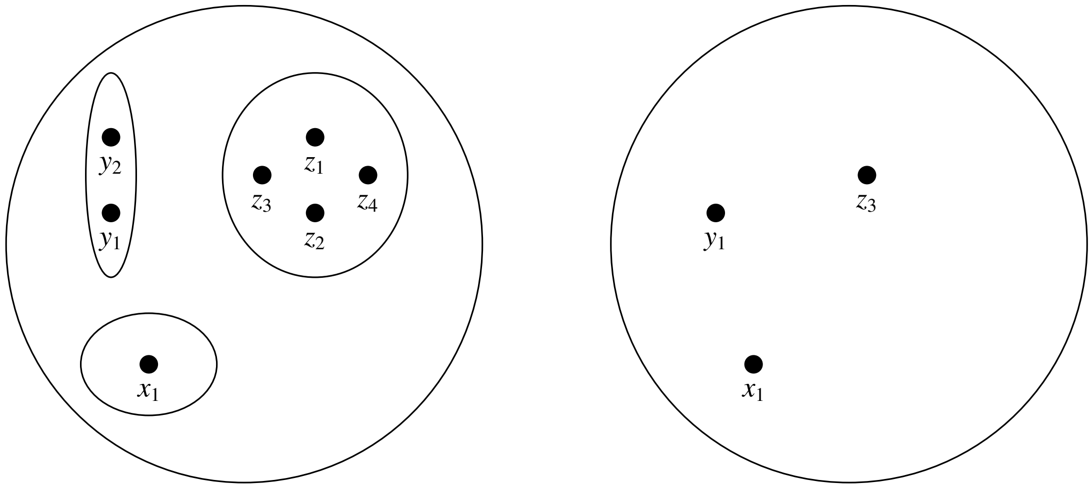
Napomena 1.1.1. Uočimo da je disjunktnost u izreci aksioma izbora nužna. Uistinu, uzmimo $X := \big\{\{1\}, \{2\}, \{1, 2\}\big\}$. Ako je B izborni skup, vrijedi da je $B \cap \{1\}$ jednočlan pa mora biti $1 \in B$. Slično, $B \cap \{2\}$ je jednočlan pa mora biti $2 \in B$. No, sada je $B \supseteq \{1, 2\}$ pa je $B \cap \{1, 2\} = \{1, 2\}$ što nije jednočlan skup. Kontradikcija! Dakle, za ovakav X nije moguće naći odgovarajući izborni skup.

Cilj ovog poglavlja je obrazložiti tvrdnju aksioma izbora, opisati njegovu uporabu, iskazati i dokazati ekvivalentne formulacije, te smjestiti aksiom izbora u „opći matematički kontekst”.

1.2 Posljedice aksioma izbora

Aksiom izbora ima brojne posljedice. Za primjer prvo opisujemo jedan podosta fantastičan scenarij, a onda i njegovu matematičku formulaciju.

Primjer 1.2.1. Zamislimo neku životinju s prebrojivo mnogo nogu (prebrojivo mnogo lijevih i prebrojivo mnogo desnih nogu), koja želi obući čarape i cipele na lijeve noge. Pretpostavimo da ima prebrojivo mnogo pari i cipela i čarapa. Može li to napraviti?



Slika 1.1: Skup X i njegov izborni skup B.

Odgovor je: ne bez aksioma izbora. Preciznije, čak i bez korištenja aksioma izbora, može iz svakog od prebrojivo mnogo parova cipela uzeti lijevu cipelu. Problem je u odabiru čarapa. Naime, bez aksioma izbora, ne može iz svakog od prebrojivo mnogo parova čarapa uzeti jednu, jer se čarape ne dijele na lijeve i desne — tu i nastaje problem!

Sličnu ilustraciju aksioma izbora je naveo Russell (vidjeti [1]).

Prije nego što damo matematičku apstrakciju te ilustracije, potrebni su nam još neki pojmovi.

Definicija 1.2.2. Neka su A i I skupovi. Svaku funkciju $f\colon I \to \mathcal{P}(A)$ nazivamo *familija skupova*. Obično pišemo A_i umjesto $f(i)$ te familiju skupova označavamo s $(A_i : i \in I)$.

Definicija 1.2.3. Neka je $(A_i\colon i \in I)$ familija skupova. Definiramo Kartezijev produkt te familije, u oznaci $\prod_{i\in I} A_i$, kao

$$\prod_{i\in I} A_i = \left\{ f\colon I \to \bigcup_{i\in I} A_i \;\middle|\; (\forall i \in I)\big(f(i) \in A_i\big) \right\}$$

Konačno, slijedi matematička apstrakcija Primjera 1.2.1.

Primjer 1.2.4. Skup $\{0,1\}^{\mathbb{N}}$ (skup svih nizova elemenata iz $\{0,1\}$) je neprazan jer npr. sadrži niz kojem su svi članovi nule.

Neka je sada, za svaki $n \in \mathbb{N}$, A_n dvočlan skup. Promatrajmo familiju $(A_n\colon n \in \mathbb{N})$. Što znamo o njenom Kartezijevom produktu?

Odgovor je: bez aksioma izbora ne možemo zaključiti da je to neprazan skup. Jedan pokušaj bi bio: kako je, za svaki $n \in \mathbb{N}$, skup A_n ekvipotentan s $\{0, 1\}$, to bi $\prod_{n\in\mathbb{N}} A_n$ trebao biti ekvipotentan s $\{0, 1\}^{\mathbb{N}}$. Što je tu krivo?

Pažljivi čitatelj će uočiti da prešutno koristimo upravo aksiom izbora — za svaki $n \in \mathbb{N}$, mi smo *izabrali* jednu bijekciju $f_n\colon A_n \to \{0, 1\}$, da bismo definirali „globalnu" bijekciju $\prod_{n\in\mathbb{N}} A_n \to \{0, 1\}^{\mathbb{N}}$.

Navedimo neke tvrdnje iz teorije skupova koje su u Zermelo–Fraenkelovoj teoriji ekvivalentne aksiomu izbora:

- (**Zornova lema**.) Neka je $(A, <)$ parcijalno uređen skup koji ima svojstvo da svaki lanac u A ima gornju među u A. Tada $(A, <)$ ima barem jedan maksimalni element.

- (**Hausdorffov princip maksimalnosti**.) Neka je $(A, <)$ parcijalno uređen skup. Tada je svaki lanac L u A podskup nekog maksimalnog lanca u A.

- (**Zermelov teorem o dobrom uređaju**.) Svaki skup se može dobro urediti: za svaki skup A postoji relacija $R \subseteq A \times A$ takva da je (A, R) dobro uređen skup.

- (**Hartogsov teorem**.) Za sve skupove A i B vrijedi $k(A) \leqslant k(B)$ ili $k(B) \leqslant k(A)$.

- (**Teorem Tarskog**.) Ako je λ beskonačni kardinalni broj, tada je $\lambda^2 = \lambda$.

- (**Russelov multiplikativni aksiom**.) Neka je $(A_i : i \in I)$ familija skupova. Ako je $\prod_{i\in I} A_i$ prazan skup, tada postoji $i \in I$ takav da je A_i prazan skup.

Aksiom izbora nije korišten samo u teoriji skupova. Često se koristi (u obliku Zornove leme) u drugim granama matematike. Navedimo još neke posljedice aksioma izbora, zajedno s granom matematike iz koje dolaze:

- (Linearna algebra) Svaki vektorski prostor ima bazu.

- (Algebra) Svako polje ima algebarski zatvoreno proširenje.

- (Algebra) Svaki prsten s jedinicom ima barem jedan maksimalni ideal.

- (Topologija) Teorem Tihonova: produkt familije kompaktnih topoloških prostora je kompaktan.

- (Analiza) Ekvivalentnost Heineove i Cauchyjeve definicije neprekidnosti funkcije.

- (Teorija mjere) Ne postoji proširenje Lebesgueove mjere definirano na cijelom $\mathcal{P}(\mathbb{R})$.

- (Funkcionalna analiza) Hahn-Banachov teorem za normirane prostore: neka je X normiran prostor i $Y < X$. Za svaki ograničeni funkcional $f_0 \in Y'$ postoji ograničeni linearni funkcional $f \in X'$ takav da je $f|_Y = f_0$ i $\|f\| = \|f_0\|$.
- (Matematička logika) Teorem kompaktnosti: Skup formula logike sudova (nad ne nužno prebrojivim jezikom) je ispunjiv ako i samo ako je ispunjiv svaki njegov konačan podskup.
- (Geometrija) Banach–Tarskijev teorem: neka su k i K kugle u $\mathbb{R}^3$. Tada postoji $n \in \mathbb{N}$ i particija $k_1, k_2, \ldots, k_n$ od k, te particija $K_1, K_2, \ldots, K_n$ od K tako da je za svaki $i = 1, 2, \ldots, n$, skup k_i izometričan s K_i.

Kao što vidimo, aksiom izbora se koristi svugdje u matematici.

Aksiom izbora je meta brojnih kritika. Najčešća kritika koja se može pronaći je da je nekonstruktivan — dokazuje postojanje nekog skupa, ali često ne znamo koji su elementi tog skupa. Također, jedna od zanimljivijih kritika se tiče upravo Banach–Tarskijevog teorema, koji se često naziva i Banach–Tarskijevim *paradoksom*. Naime, iz Banach–Tarskijevog teorema slijedi da postoji particija jedinične kugle u konačno mnogo skupova, takvih da se iz tih skupova translacijama i rotacijama mogu dobiti dvije jedinične kugle. Ne znamo precizno opisati sve dijelove koje dobijemo takvom dekompozicijom jedinične kugle. Ono što je ključno je da su neki dijelovi *neizmjerivi*: ne možemo govoriti o volumenu tih dijelova. Naime, translacije i rotacije čuvaju volumen, pa kada bi svi dijelovi bili izmjerivi (tj. imali volumen), ne bismo od jedne jedinične kugle, koristeći samo translacije i rotacije, mogli dobiti dvije.

1.3 Ekvivalentne formulacije

U literaturi možemo naći različite formulacije tvrdnje aksioma izbora. U ovom potpoglavlju nam je cilj navesti neke od njih i dokazati ekvivalentnost tih formulacija s onom koju smo naveli kao Aksiom 0.0.2. Započnimo s formulacijom iz [3] (uz malu modifikaciju na nepraznost familije).

Tvrdnja 1.3.1. Neka je $(A_i : i \in I)$ familija u parovima disjunktnih nepraznih skupova. Tada postoji skup B takav da je za svaki $i \in I$ skup $B \cap A_i$ jednočlan.

Funkcije koje se pojavljuju u sljedećim tvrdnjama obično zovemo *funkcijama izbora*.

Tvrdnja 1.3.2. Neka je $(A_i : i \in I)$ familija u parovima disjunktnih nepraznih skupova. Tada postoji $f \colon I \to \bigcup_{i \in I} A_i$ takva da za svaki $i \in I$ vrijedi $f(i) \in A_i$.

Tvrdnja 1.3.3. Za svaki skup nepraznih skupova X postoji funkcija $f \colon X \to \bigcup_{A \in X} A$ takva da za sve $A \in X$ vrijedi $f(A) \in A$.

Tvrdnja 1.3.4. Neka je A skup. Tada postoji $f\colon \mathcal{P}(A) \setminus \{\emptyset\} \to A$ takva da je $f(B) \in B$ za sve $B \in \mathcal{P}(A) \setminus \{\emptyset\}$.

Tvrdnja 1.3.5. Neka je A skup i $\mathcal{A}$ particija skupa A. Tada postoji $f\colon \mathcal{A} \to A$ takva da je $f(B) \in B$ za sve $B \in \mathcal{A}$.

Teorem 1.3.6. *Aksiom 0.0.2 i tvrdnje 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5 su ekvivalentne.*

Dokaz. Dokazujemo teorem pomoću lanca implikacija.
$\boxed{0.0.2 \Rightarrow 1.3.1}$ Neka je $(A_i : i \in I)$ familija u parovima disjunktnih nepraznih skupova. Definiramo skup $X = \{A_i \mid i \in I\}$. Primijetimo da je X skup u parovima disjunktnih nepraznih skupova pa po pretpostavci postoji skup B takav da je $B \cap Y$ jednočlan za svaki $Y \in X$. Iz definicije skupa X slijedi da to upravo znači da je $B \cap A_i$ jednočlan za svaki $i \in I$.
$\boxed{1.3.1 \Rightarrow 1.3.2}$ Neka je $(A_i : i \in I)$ familija u parovima disjunktnih nepraznih skupova. Po pretpostavci postoji skup B takav da je $B \cap A_i$ jednočlan za svaki $i \in I$. Definiramo relaciju $f := \bigcup_{i \in I} \big(\{i\} \times (B \cap A_i)\big)$. Pokažimo da f ima funkcijsko svojstvo. Neka je $i \in I$. Kako $B \cap A_i \neq \emptyset$, to i $\{i\} \times (B \cap A_i) \neq \emptyset$. Dakle, $i \in \mathcal{D}_f$. Pretpostavimo da za neki $i \in I$ vrijedi $(i, x), (i, y) \in f$. Po definiciji od f slijedi $x, y \in B \cap A_i$. S obzirom da je $B \cap A_i$ jednočlan, slijedi $x = y$. Dakle, f uistinu ima funkcijsko svojstvo. Uočimo da također vrijedi i $f(i) \in A_i$ za sve $i \in I$ pa je f tražena funkcija.
$\boxed{1.3.2 \Rightarrow 1.3.3}$ Neka je X skup nepraznih skupova. Označimo $I := X$, $A_Y := Y \times \{Y\}$ i promatramo familiju $(A_i : i \in I) = (A_Y : Y \in X)$. To je familija u parovima disjunktnih nepraznih skupova pa po pretpostavci postoji $f\colon I \to \bigcup_{i \in I} A_i$ takva da je $f(i) \in A_i$ za sve $i \in I$. Pogledamo li definiciju skupa I vidimo da to upravo znači da je $f(Y) \in Y \times \{Y\}$ za sve $Y \in X$. Definiramo $g\colon X \to \bigcup_{Y \in X} Y$ s $g := \pi_1 \circ f$, gdje je $\pi_1\colon \bigcup_{i \in I} A_i \to \bigcup_{Y \in X} Y$ definirana s $\pi_1(x, y) := x$ (dakle, standardna projekcija). Ta funkcija zadovoljava $g(Y) \in Y$ za sve $Y \in X$ jer je $g(Y) = (\pi_1 \circ f)(Y) = \pi_1\big(f(Y)\big) \in Y$.
$\boxed{1.3.3 \Rightarrow 1.3.4}$ Uočimo da je $\mathcal{P}(A) \setminus \{\emptyset\}$ skup nepraznih skupova pa po pretpostavci postoji $f\colon \mathcal{P}(A) \setminus \{\emptyset\} \to \bigcup_{Y \in \mathcal{P}(A) \setminus \{\emptyset\}} Y$ takva da je $f(B) \in B$ za sve $B \in \mathcal{P}(A) \setminus \{\emptyset\}$. Još samo treba uočiti da je $\bigcup_{Y \in \mathcal{P}(A) \setminus \{\emptyset\}} Y = A$. Za $A = \emptyset$ ta tvrdnja trivijalno vrijedi jer je $\mathcal{P}(\emptyset) \setminus \{\emptyset\} = \emptyset$. Pretpostavimo da je $A \neq \emptyset$. Uočimo da je $Y \subseteq A$ za sve $Y \in \mathcal{P}(A) \setminus \{\emptyset\}$, što znači da je $\bigcup_{Y \in \mathcal{P}(A) \setminus \{\emptyset\}} Y \subseteq A$. Obratno, kako je $A \in \mathcal{P}(A) \setminus \{\emptyset\}$ za $A \neq \emptyset$, vrijedi i $A \subseteq \bigcup_{Y \in \mathcal{P}(A) \setminus \{\emptyset\}} Y$.
$\boxed{1.3.4 \Rightarrow 1.3.5}$ Po pretpostavci postoji $f\colon \mathcal{P}(A) \setminus \{\emptyset\} \to A$ takva da je $f(B) \in B$ za sve $B \in \mathcal{P}(A) \setminus \{\emptyset\}$. Kako je $\mathcal{A} \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$, za $g := f|_{\mathcal{A}}$ vrijedi $g(B) \in B$ za sve $B \in \mathcal{A}$.
$\boxed{1.3.5 \Rightarrow 0.0.2}$ Neka je X skup u parovima disjunktnih nepraznih skupova. Uočimo da je tada X particija skupa $S := \bigcup_{Y \in X} Y$. Po pretpostavci postoji $f\colon X \to S$ takva da je $f(Y) \in Y$ za sve $Y \in X$. Definiramo skup $B := \{f(Y) \mid Y \in X\}$. Iz definicije je odmah jasno da je $B \cap Y \neq \emptyset$ za sve $Y \in X$. Tvrdimo da su svi presjeci jednočlani. Pretpostavimo suprotno, tj. postoji $Y' \in X$ takav da postoje $y_1, y_2 \in B \cap Y'$, $y_1 \neq y_2$. Iz definicije skupa B to znači da postoje $Y_1, Y_2 \in X$ takvi da je $f(Y_1) = y_1$ i $f(Y_2) = y_2$. Kako je $y_1 \in Y_1$ i

$y_1 \in B \cap Y' \subseteq Y'$, slijedi da je $y_1 \in Y_1 \cap Y'$. No to znači da je $Y_1 = Y'$! Naime, X je skup disjunktnih skupova, a Y_1 i Y' imaju zajednički element. Analogno dobijemo i $Y_2 = Y'$. Drugim riječima, $Y_1 = Y_2$, što znači da je $y_1 = f(Y_1) = f(Y_2) = y_2$. Kontradikcija! Dakle, $B \cap Y$ je jednočlan skup za sve $Y \in X$. □

1.4 Primjer korištenja aksioma izbora: Vitalijev skup

Već smo nekoliko puta spomenuli da je naglasak na Zornovoj lemi jer se češće koristi nego aksiom izbora u svome najčišćem obliku. No, aksiom izbora se ipak i u tom obliku koristi za dokaz nekih tvrdnji. U ovom potpoglavlju se bavimo jednom takvom tvrdnjom. Iako tvrdnja tematski pripada ovom poglavlju, u dokazu koristimo neke pojmove koje uvodimo tek poslije u ovom radu, npr. koristimo *relaciju*. Od čitatelja se očekuje osnovno znanje pojmova iz teorije skupova i teorije mjere da bi mogao pratiti dokaz.

Tvrdnja 1.4.1. Ne postoji proširenje Lebesgueove mjere definirano na cijelom $\mathcal{P}(\mathbb{R})$.

Dokaz. Pretpostavimo suprotno, odnosno da postoji mjera $m\colon \mathcal{P}(\mathbb{R}) \to [0, +\infty]$ koja ima sva svojstva koje ima Lebesgueova mjera. Specijalno, m mora imati sljedeća svojstva:

(i) Za sve $a, b \in \mathbb{R}$, $a \leqslant b$, je $m([a, b]) = b - a$.

(ii) $m(\emptyset) = 0$.

(iii) Neka je $(A_n : n \in \mathbb{N})$ prebrojiva familija u parovima disjunktnih podskupova od $\mathbb{R}$. Tada vrijedi $m\left(\bigcup_{n=0}^{\infty} A_n\right) = \sum_{n=0}^{\infty} m(A_n)$.

(iv) Za sve $x \in \mathbb{R}$ i sve $A \subseteq \mathbb{R}$ vrijedi $m(A + x) = m(A)$.

Neka su $A, B \subseteq \mathbb{R}$ takvi da je $A \subseteq B$. Tada je

$$m(B) = m\big(A \cup (B \setminus A)\big) = m(A) + m(B \setminus A) \geqslant m(A), \tag{1.1}$$

gdje je druga jednakost posljedica svojstva (iii), a nejednakost vrijedi jer je $m(B \setminus A) \geqslant 0$ po definiciji mjere.

Na $\mathbb{R}$ definiramo relaciju $\sim$ pomoću

$$a \sim b :\Leftrightarrow b - a \in \mathbb{Q}.$$

Dokažimo da je $\sim$ relacija ekvivalencije.

- (Refleksivnost) Neka je $x \in \mathbb{R}$. Tada je $x - x = 0 \in \mathbb{Q}$ pa je $x \sim x$.

- (Simetričnost) Neka su $x, y \in \mathbb{R}$ takvi da je $x \sim y$. Dakle, vrijedi $y - x \in \mathbb{Q}$. No, tada je i $x - y = -(y - x) = (-1)(y - x) \in \mathbb{Q}$ što povlači $y \sim x$.

- (Tranzitivnost) Neka su $x, y, z \in \mathbb{R}$ takvi da je $x \sim y$ i $y \sim z$. Zapišimo $z - x = (z - y) + (y - x)$. Kako su $y - x \in \mathbb{Q}$ i $z - y \in \mathbb{Q}$, to je i $z - x \in \mathbb{Q}$. Dakle, $x \sim z$.

Za $x \in \mathbb{R}$ označimo s K_x pripadnu klasu ekvivalencije koja sadrži x. Uočimo da je $\lfloor x \rfloor \in \mathbb{Q}$ pa je $x - \lfloor x \rfloor \in K_x \cap [-1, 1]$. Dakle, svaka klasa ekvivalencije ima barem jedan element koji se nalazi u $[-1, 1]$.

Po aksiomu izbora slijedi da postoji izborni skup za $\mathbb{R}/_\sim$, koji ćemo označiti s A. Uočimo da možemo postići da je $A \subseteq [-1, 1]$ (iz svake klase ekvivalencije izaberemo jednog njenog predstavnika koji se nalazi u $[-1, 1]$). Skup A nazivamo i *Vitalijev skup*.

Znamo da je $\mathbb{Q} \cap [-2, 2]$ prebrojiv; poredajmo mu elemente u niz $(q_n)_{n\in\mathbb{N}}$. Za sve $n \in \mathbb{N}$ definiramo $A_n := A + q_n$. Očito $A_n \subseteq [-3, 3]$.

Pretpostavimo da su $m, n \in \mathbb{N}$, $m \neq n$. Dokažimo da onda $A_m \cap A_n = \emptyset$. Uistinu, pretpostavimo li suprotno, postoji neki $x \in A_m \cap A_n$. Tada postoje $a, b \in A$ takvi da je $x = a + q_m$ i $x = b + q_n$. To povlači da je $a + q_m = b + q_n$, tj. $b - a = q_m - q_n \in \mathbb{Q}$. Dakle, $a \sim b$, što znači da je $K_a = K_b$. No, po konstrukciji od A smo iz svake klase ekvivalencije izabrali samo jedan element pa je $a = b$. Iz $x = a + q_m = b + q_n$ sada lako slijedi $q_m = q_n$ pa i $m = n$, kontradikcija. Dakle, $A_m \cap A_n = \emptyset$ za sve $m, n \in \mathbb{N}$, $m \neq n$.

Sada je

$$\sum_{n=0}^{\infty} m(A_n) = m\left(\bigcup_{n=0}^{\infty} A_n\right) \leqslant m([-3, 3]) = 6,$$

gdje prva jednakost slijedi iz svojstva (iii), nejednakost $m\left(\bigcup_{n=0}^{\infty} A_n\right) \leqslant m([-3, 3])$ je posljedica nejednakosti (1.1) (jer je $A_n \subseteq [-3, 3]$ za sve $n \in \mathbb{N}$ pa je i $\bigcup_{n=0}^{\infty} A_n \subseteq [-3, 3]$), a zadnja jednakost slijedi iz svojstva (i).

Po svojstvu (iv) znamo da je $m(A_n) = m(A)$ za sve $n \in \mathbb{N}$. Drugim riječima,

$$\sum_{n=0}^{\infty} m(A) = \sum_{n=0}^{\infty} m(A_n) \leqslant 6$$

(bitno je samo da ta mjera nije ∞) pa mora biti $m(A) = 0$ te

$$\sum_{n=0}^{\infty} m(A) = 0. \tag{1.2}$$

S druge strane, neka je $x \in [-1, 1]$. Po definiciji od A postoji $a \in A$ takav da je ujedno $a \sim x$. Dakle, vrijedi $x - a \in \mathbb{Q}$ i, zato što su oba iz segmenta $[-1, 1]$, vrijedi i $x - a \in \mathbb{Q} \cap [-2, 2]$. Drugim riječima, $x = a + q_{n_0}$ za neki $n_0 \in \mathbb{N}$ pa je $x \in A_{n_0}$ po definiciji skupa A_{n_0}. Iz ovoga slijedi da je $[-1,1] \subseteq \bigcup_{n=0}^{\infty} A_n$. Sličnim pozivanjem na svojstva kao i prije dobivamo

$$\sum_{n=0}^{\infty} m(A) = \sum_{n=0}^{\infty} m(A_n) = m\left(\bigcup_{n=0}^{\infty} A_n\right) \geqslant m([-1,1]) = 2,$$

što je očita kontradikcija s (1.2). Dakle, pretpostavka da mjera m s opisanim svojstvima postoji je kriva, što smo i trebali dokazati. $\square$

Poglavlje 2

Zornova lema

2.1 Uvodno o Zornovoj lemi

U ovoj sekciji nam je cilj precizno izreći i rastumačiti Zornovu lemu. Najprije definiramo nekoliko pojmova.

Definicija 2.1.1. Neka je A skup. *Relacijom na* A nazivamo bilo koji podskup Kartezijevog produkta $A \times A$.

Napomena 2.1.2. Neka je A skup i R relacija na A. Često umjesto $(x, y) \in R$ pišemo $x\ R\ y$, a umjesto $(x, y) \notin R$ pišemo $x \not R\ y$.

Definicija 2.1.3. Neka je A skup i R relacija na A sa sljedećim svojstvima:

- (Irefleksivnost) Za sve $x \in A$ vrijedi $x \not R\ x$.
- (Tranzitivnost) Za sve $x, y, z \in A$, ako vrijedi $x\ R\ y$ i $y\ R\ z$, onda vrijedi i $x\ R\ z$.

Tada kažemo da je R *relacija parcijalnog uređaja* te da je (A, R) *parcijalno uređen skup*.

Napomena 2.1.4. Često ćemo relacije parcijalnog uređaja označavati s $<$, $\prec$ i slično. Također, definiramo pomoćne relacije $\leqslant$, $\preccurlyeq$ s

$$x \leqslant y :\Leftrightarrow (x < y) \vee (x = y),$$
$$x \preccurlyeq y :\Leftrightarrow (x \prec y) \vee (x = y).$$

Primjer 2.1.5. Na skupu prirodnih brojeva, $\mathbb{N}$, definiramo relaciju $<$ na sljedeći način:

$$x < y :\Leftrightarrow (\exists z \in \mathbb{N} \setminus \{0\})(x + z = y).$$

Jasno, ovu relaciju već znamo kao *prirodni uređaj na* $\mathbb{N}$. Dokažimo da je $<$ relacija parcijalnog uređaja.

- (Irefleksivnost) Neka je $x \in \mathbb{N}$. Kada bi bilo $x < x$, postojao bi $z \in \mathbb{N} \setminus \{0\}$ takav da je $x + z = x$. No iz ovoga odmah slijedi $z = 0$, što je očita kontradikcija. Dakle, $x \nless x$.
- (Tranzitivnost) Neka su $x, y, z \in \mathbb{N}$ takvi da $x < y$ i $y < z$. Tada postoje $u, v \in \mathbb{N} \setminus \{0\}$ takvi da $x + u = y$ i $y + v = z$. Zbrajanjem tih jednadžbi dobivamo $x + u + y + v = y + z$, tj. $x + (u + v) = z$. Kako je $u + v \in \mathbb{N} \setminus \{0\}$ slijedi $x < z$.

Definicija 2.1.6. Neka je $(A, <)$ parcijalno uređen skup koji ima dodatno svojstvo da za sve $x, y \in A$ vrijedi

$$x < y \quad \vee \quad x = y \quad \vee \quad y < x. \tag{2.1}$$

Ovo svojstvo nekada nazivamo i *linearnost* ili *totalnost*. Tada $<$ nazivamo *relacijom linearnog uređaja*, a za $(A, <)$ kažemo da je *linearno uređen skup*.

Napomena 2.1.7. U svjetlu Napomene 2.1.4, uvjet (2.1) se može iskazati i kao

$$x \leqslant y \quad \vee \quad y < x,$$

što je često korisno jer smanjuje broj slučajeva pri dokazivanju.

Definicija 2.1.8. Neka je $(A, <)$ parcijalno uređen skup i neka je $S \subseteq A$ takav da za sve $x, y \in S$ vrijedi

$$x \leqslant y \quad \vee \quad y < x$$

(dakle, vrijedi linearnost uređaja $(<) \cap (S \times S)$ na S). Tada za S kažemo da je *lanac u A*.

Primjer 2.1.9. Neka je $A := \{1, 2\}$. Tada je $\mathcal{P}(A) = \big\{\emptyset, \{1\}, \{2\}, \{1, 2\}\big\}$. Na $\mathcal{P}(A)$ definiramo relaciju $\prec$ s $x \prec y :\Leftrightarrow x \subset y$. Lako se pokaže da je $\prec$ relacija parcijalnog uređaja. Međutim, $\prec$ *nije* relacija linearnog uređaja. Uistinu, uočimo da je $\{1\} \neq \{2\}$, te ne vrijedi $\{1\} \prec \{2\}$ niti $\{2\} \prec \{1\}$.

Promotrimo sada $S := \big\{\emptyset, \{1\}, \{1, 2\}\big\} \subseteq \mathcal{P}(A)$. Uočimo da za sve $x, y \in S$ vrijedi $x \subseteq y$ ili $y \subset x$. Drugim riječima, $(\prec) \cap (S \times S)$ je linearan na S pa je S lanac u $\mathcal{P}(A)$.

Jasno, lako možemo naći još neke lance u $\mathcal{P}(A)$. Recimo, $\big\{\{1\}, \{1, 2\}\big\}$, $\big\{\emptyset, \{1, 2\}\big\}$, $\emptyset$ su sve lanci u $\mathcal{P}(A)$.

Definicija 2.1.10. Neka je $(A, <)$ parcijalno uređen skup. Za $x \in A$ kažemo da je *maksimalan* (*minimalan*) ako ne postoji $y \in A$ takav da vrijedi $x < y$ ($y < x$). Za $x \in A$ kažemo da je *najveći* (*najmanji*) ako za sve $y \in A$ vrijedi $y \leqslant x$ ($x \leqslant y$).

Napomena 2.1.11. Iz definicije je jasno da je svaki najveći element ujedno i maksimalni. Obrat ne vrijedi. Očit kontraprimjer je $(\{1, 2\}, \emptyset)$. U ovom slučaju su i 1 i 2 maksimalni elementi, ali ovakav parcijalno uređeni skup ne posjeduje najveći element.

Čak i ako parcijalno uređeni skup posjeduje jedinstven maksimalan element, ne mora vrijediti da posjeduje i najveći element. Za primjer uzmimo $(\mathbb{R} \cup \{i\}, <)$, gdje je $<$ standardni uređaj na skupu realnih brojeva. Drugim riječima, u ovakvom parcijalno uređenom skupu i nije *usporediv* niti s jednim elementom, tj. ni za koji $x \in \mathbb{R}$ ne vrijedi ni $x < i$ ni $i < x$. Iz ovoga je jasno da je i maksimalni element, no također je jasno da nije najveći element. Nadalje, za sve $x \in \mathbb{R}$ vrijedi $x < x + 1$ pa niti jedan $x \in \mathbb{R}$ nije maksimalan. Dakle, i je jedinstveni maksimalni element, ali nije najveći element.

Propozicija 2.1.12. Neka je A konačni neprazni skup. Neka je $<$ linearni uređaj na A. Tada $(A, <)$ ima najveći element.

Dokaz. Dokaz provodimo principom matematičke indukcije po broju elemenata od A, koji ćemo označiti s n.

Baza je $n = 1$. Tada je $A = \{a\}$ i a je očito najveći element.

Pretpostavimo da tvrdnja vrijedi za neki $n \in \mathbb{N} \setminus \{0\}$, za sve skupove s n elemenata. Neka A ima $n + 1$ elemenata i neka je $a \in A$ neki njegov element. Definiramo $A' := A \setminus \{a\}$. Sada A' ima n elemenata pa iz pretpostavke indukcije slijedi da ima najveći element; označimo ga s a'. Očito $a' \neq a$ jer $a \notin A'$ pa iz linearnosti od $<$ slijedi da je ili $a' < a$ ili $a < a'$. U prvom slučaju je a najveći element u A. Uistinu, neka je $b \in A$. Ako je $b = a$, trivijalno je $b \leqslant a$. Inače je $b \in A'$ pa je $b \leqslant a'$ jer je a' najveći element u A'. Iz tranzitivnosti sada slijedi $b < a$. Ako je pak $a < a'$, onda je očito a' najveći element u A.

Po principu matematičke indukcije sada slijedi tvrdnja. □

Definicija 2.1.13. Neka je $(A, <)$ parcijalno uređen skup i $B \subseteq A$. Za element $x \in A$ kažemo da je *gornja međa* (*donja međa*) skupa B ako za sve $y \in B$ vrijedi $y \leqslant x$ ($x \leqslant y$).

Konačno, ponovimo tvrdnju Zornove leme.

Teorem 0.0.1. Neka je $(A, <)$ parcijalno uređen skup koji ima svojstvo da svaki lanac u A ima gornju među u A. Tada $(A, <)$ ima barem jedan maksimalni element.

Naš sljedeći cilj je dokazati Zornovu lemu. Također, cilj je dati što „elementarniji" dokaz, koji koristi što manje „jakih" tvrdnji teorije skupova. Recimo, jedan od glavnih ciljeva je izbjeći izravno korištenje *ordinala*. Kao veliku pomoć navodimo referencu [2].

2.2 Prema dokazu Zornove leme

Kada krenemo proučavati primjere parcijalno uređenih skupova, počnemo uočavati da se neki na određeni način „ponavljaju". Konkretno, dajmo jedan primjer tog „ponavljanja".

Primjer 2.2.1. Promotrimo parcijalno uređene skupove $S_1 := \big(\{1, 2\}, \{(1, 2)\}\big)$ i $S_2 := \big(\{3, 4\}, \{(3, 4)\}\big)$. Možemo uočiti da su oni na određeni način *slični*. Preciznije, 1 u S_1

ima istu ulogu kao 3 u S_2, dok 2 u S_1 ima istu ulogu kao 4 u S_2. Malo „računarski" rečeno, ustvari promatramo dvije različite „implementacije" iste stvari.

Dodajmo u promatranje parcijalno uređeni skup $S_3 := \big(\{1,2\},\emptyset\big)$. Njegovi elementi su 1 i 2, isti kao i elementi od S_1 (točnije rečeno, to su elementi „skupovnog dijela" parcijalno uređenih skupova S_1 i S_3). S druge strane, S_1 i S_3 su na određeni način puno manje *slični* nego S_1 i S_2. Drugim riječima, 1 i 2 u S_1 nemaju iste uloge kao 1 i 2 u S_3.

Cijelu raspravu vezanu za Primjer 2.2.1 možemo formalizirati.

Definicija 2.2.2. Neka su $(A,<)$ i $(B,\prec)$ parcijalno uređeni skupovi. Kažemo da $f\colon A\to B$ *čuva uređaj* ako vrijedi

$$(\forall x,y\in A)\big(x<y\Rightarrow f(x)\prec f(y)\big).$$

Definicija 2.2.3. Neka su $(A,<)$ i $(B,\prec)$ parcijalno uređeni skupovi. Kažemo da su *slični* ako postoji bijekcija $f\colon A\to B$ (koju još nazivamo *sličnost*) takva da f i f^{-1} čuvaju uređaj.

Napomena 2.2.4. Pomoću Primjera 2.2.1 možemo uočiti motivaciju iza Definicije 2.2.3. Naime, svakom $x\in A$ želimo pridružiti $y\in B$ takav da x u $(A,<)$ ima istu ulogu kao y u $(B,\prec)$. Pridruživanje je naravno izvedeno uporabom funkcije f, a svojstvo da f i f^{-1} čuvaju uređaj osigurava da će x u $(A,<)$ imati istu ulogu kao y u $(B,\prec)$.

Napomena 2.2.5. Uvjet da f^{-1} čuva uređaj je zaista nezavisan od ostalih uvjeta u Definiciji 2.2.3. Uistinu, promatrajmo opet S_1 i S_3 iz Primjera 2.2.1, te uvedimo $A_1 := \{1,2\}$, $R_1 := \{(1,2)\}$, $A_3 := \{1,2\}$, $R_3 := \emptyset$ (dakle, vrijedi $S_1 = (A_1,R_1)$ i $S_3 = (A_3,R_3)$).

Definirajmo bijekciju $f\colon A_3\to A_1$ sa $f(1) := 1$, $f(2) := 2$ (drugim riječima, f je identiteta na $\{1,2\}$) i f trivijalno čuva uređaj jer ne postoje $x,y\in A_3$ takvi da $x\ R_3\ y$. S druge strane, $1\ R_1\ 2$, ali $1\ \not R_3\ 2$, pa $f^{-1}(1)\ \not R_3\ f^{-1}(2)$, odnosno f^{-1} ne čuva uređaj.

U ovom primjeru također možemo vidjeti koliko je važan sveukupan kontekst; naime, i f i f^{-1}, kada ih proučavamo samo kao funkcije, su identitete na $A_1 = A_3$. Ono po čemu se razlikuju u smislu „čuvanja uređaja" je da f ide sa S_3 u S_1, a f^{-1} ide sa S_1 u S_3, pri čemu S_1 i S_3 nisu parcijalno uređeni istom relacijom.

Napomena 2.2.6. Sličnost ne mora biti jedinstvena. Na primjer, neka je S_3 kao iz Primjera 2.2.1 i $S_4 := (\{3,4\},\emptyset)$. Lako se vidi da su $g_1\colon\{1,2\}\to\{3,4\}$, definirana s $g_1(1) := 3$, $g_1(2) := 4$, i $g_2\colon\{1,2\}\to\{3,4\}$, definirana s $g_2(1) := 4$, $g_2(2) := 3$, dvije različite sličnosti između S_3 i S_4.

Za malo manje trivijalni primjer promatrajmo $(\mathbb{Z},<)$, gdje je $<$ uobičajeni parcijalni uređaj nad $\mathbb{Z}$. Neka je $m\in\mathbb{Z}$ i definirajmo $f_m\colon\mathbb{Z}\to\mathbb{Z}$ s $f_m(n) = n+m$. Lako se vidi da je f_m bijekcija, da je $f_m^{-1}(n) = n-m$, da f_m i f_m^{-1} čuvaju uređaj, te da je $m\mapsto f_m$ injekcija. Drugim riječima, našli smo beskonačno mnogo sličnosti između $(\mathbb{Z},<)$ i $(\mathbb{Z},<)$.

Propozicija 2.2.7. Neka su $(A, <)$ i $(B, \prec)$ slični parcijalno uređeni skupovi i neka je $f : A \to B$ (neka) sličnost.

1) $x \in A$ je maksimalan (minimalan) element u $(A, <)$ ako i samo ako je $f(x)$ maksimalan (minimalan) element u $(B, \prec)$.

2) $x \in A$ je najveći (najmanji) element u $(A, <)$ ako i samo ako je $f(x)$ najveći (najmanji) element u $(B, \prec)$.

3) $S \subseteq A$ ima gornju (donju) među u A ako i samo ako $f[S]$[1] ima gornju (donju) među u B.

4) $S \subseteq A$ je lanac u A ako i samo ako je $f[S]$ lanac u B.

Dokaz.

1) Dokazat ćemo samo varijantu za maksimalne elemente, za minimalne je dokaz analogan.

   Neka je $x \in A$ maksimalan. Pretpostavimo da $f(x)$ nije maksimalan. To znači da postoji $y \in B$ takav da je $f(x) \prec y$. Zato što f^{-1} čuva uređaj, $f^{-1}\big(f(x)\big) < f^{-1}(y)$, tj. $x < f^{-1}(y)$. No to je nemoguće jer je x maksimalan. Dakle, $f(x)$ mora biti maksimalan.

   Pretpostavimo sada da je $x \in A$ takav da je $f(x)$ maksimalan. Pretpostavimo da x nije maksimalan. Tada postoji $y \in A$ takav da $x < y$. Kako f čuva uređaj sada vrijedi $f(x) \prec f(y)$. No to je kontradikcija s pretpostavkom da je $f(x)$ maksimalan. Dakle, x mora biti maksimalan.

2) Dokazat ćemo samo varijantu za najveće elemente, za najmanje je dokaz analogan.

   Neka je $x \in A$ najveći element. Neka je $z \in B$ proizvoljan. Zato što je f surjekcija, postoji $y \in A$ takav da $f(y) = z$. S obzirom da je x najveći element, vrijedi $y \leqslant x$. Zato što f čuva uređaj vrijedi $f(y) \preccurlyeq f(x)$. Dakle, $z \preccurlyeq f(x)$. Zbog proizvoljnosti od $z \in B$ zaključujemo da je $f(x)$ najveći element.

   Neka je sada $x \in A$ takav da je $f(x)$ najveći element. Neka je $y \in A$ proizvoljan. Sigurno je $f(y) \preccurlyeq f(x)$. No, f^{-1} čuva uređaj pa je $f^{-1}\big(f(y)\big) \preccurlyeq f^{-1}\big(f(x)\big)$, tj. $y \leqslant x$. Slijedi da x mora biti najveći element.

3) Dokazat ćemo samo varijantu za gornju među, za donju među dokaz je analogan.

   Neka je $S \subseteq A$ takav da ima gornju među u A. Drugim riječima, postoji $m \in A$ takav da je $x \leqslant m$ za sve $x \in S$. Neka je $y \in f[S]$. To po definiciji znači da postoji $x \in S$

[1] Za skup $S \subseteq \mathrm{Dom}(f)$ definiramo $f[S] := \{f(s) \mid s \in S\}$.

takav da je $y = f(x)$. No, iz $x \preccurlyeq m$ slijedi $f(x) \preccurlyeq f(m)$ jer f čuva uređaj. Dakle, za sve $y \in f[S]$ vrijedi $y \preccurlyeq f(m)$ pa je $f(m)$ gornja međa od $f[S]$ u B.

S druge strane, neka je $S \subseteq A$ takav da $f[S]$ ima gornju među u B. Dakle, postoji $n \in B$ takav da je $y \preccurlyeq n$ za sve $y \in f[S]$. Neka je $x \in S$. Tada je $f(x) \in f[S]$ što znači da vrijedi $f(x) \preccurlyeq n$. Kako f^{-1} čuva uređaj, vrijedi $f^{-1}\big(f(x)\big) \preccurlyeq f^{-1}(n)$, tj. $x \preccurlyeq f^{-1}(n)$. Dakle, $f^{-1}(n)$ je gornja međa od S.

4) Neka je $S \subseteq A$ lanac u A. Neka su $y_1, y_2 \in f[S]$. Tada postoje $x_1, x_2 \in S$ takvi da je $y_1 = f(x_1)$, $y_2 = f(x_2)$. Zato što je S lanac, vrijedi $x_1 < x_2$, $x_1 = x_2$, ili $x_2 < x_1$. Ako je $x_1 < x_2$ onda je $f(x_1) \prec f(x_2)$ jer f čuva uređaj, a iz toga odmah slijedi $y_1 \prec y_2$. Analogno, ako je $x_2 < x_1$, onda je $y_2 \prec y_1$. Ako je $x_1 = x_2$ onda je trivijalno $f(x_1) = f(x_2)$ jer je to upravo funkcijsko svojstvo, te je $y_1 = y_2$. Dakle, vrijedi $y_1 \prec y_2$, $y_1 = y_2$, ili $y_2 \prec y_1$, te je $f[S]$ lanac.

Pretpostavimo da je $f[S]$ lanac. S obzirom da je $S = f^{-1}\big[f[S]\big]$ (jer je f bijekcija) po prethodnom (jer je f^{-1} također sličnost) zaključujemo da je S lanac. □

Napomena 2.2.8. Uočimo da smo mogli koristiti činjenicu da je f^{-1} također sličnost i u dokazu tvrdnji 1), 2) i 3). No, ovdje smo se odlučili za varijantu u kojoj se što direktnije dokazuju te tvrdnje.

Korolar 2.2.9. *Ako je $(A, <)$ linearno uređen skup sličan $(B, \prec)$, tada je i $(B, \prec)$ linearno uređen skup.*

Dokaz. Slijedi direktno iz Propozicije 2.2.7, tvrdnje 4) jer je A lanac u A i $f[A] = B$ zbog surjektivnosti od f. □

Slijedi jedna zanimljiva „klasifikacijska” tvrdnja: bez puno smanjenja općenitosti možemo pretpostaviti da je bilo koji parcijalni uređaj upravo $\subset$. Ta tvrdnja može uvelike pomoći kod nekih dokaza jer nam je relaciju $\subset$ jednostavnije promatrati nego općenite relacije; na primjer, gornja međa lanca će u tom slučaju gotovo uvijek biti njegova unija.

Lema 2.2.10. *Neka je $(A, <)$ parcijalno uređen skup. Tada postoji $\mathcal{A} \subseteq \mathcal{P}(A)$ takav da je $(A, <)$ sličan $(\mathcal{A}, \subset)$.*

Dokaz. Neka je $x \in A$. Definiramo

$$\overline{x} := \{y \in A \mid y \leqslant x\}. \tag{2.2}$$

Ovime smo ustvari definirali jedno preslikavanje $\overline{\cdot}\colon A \to \mathcal{P}(A)$. Neka je $\mathcal{A}$ slika tog preslikavanja. Dokazat ćemo da je $\overline{\cdot}$ sličnost između $(A, <)$ i $(\mathcal{A}, \subset)$.

Pokažimo injektivnost. Neka su $x, y \in A$ takvi da je $\overline{x} = \overline{y}$. Iz (2.2) je jasno da je $y \in \overline{y}$. Iz $\overline{y} = \overline{x}$ slijedi $y \in \overline{x}$. Iz (2.2) sada slijedi $y \leqslant x$. Analogno dobijemo da vrijedi i $x \leqslant y$.

Pretpostavimo da je $x \neq y$. Tada vrijedi $y < x$ i $x < y$ pa iz tranzitivnosti relacije $<$ slijedi i $y < y$. To je kontradikcija s činjenicom da je relacija $<$ irefleksivna. Dakle, mora biti $x = y$, odnosno funkcija $\overline{\cdot}$ je injekcija.

Surjektivnost slijedi iz definicije $\mathcal{A}$ kao slike od $\overline{\cdot}$.

Pokažimo da $\overline{\cdot}$ čuva uređaj. Neka su $x, y \in A$ takvi da vrijedi $x < y$. Neka je $z \in \overline{x}$. Tada za $z \neq x$ iz (2.2) slijedi $z < x$ i $x < y$, tj. zbog tranzitivnosti vrijedi $z < y$, te $z \in \overline{y}$. Za $z = x$ je trivijalno $z < y$, te $z \in \overline{y}$. Slijedi da je $\overline{x} \subseteq \overline{y}$. No, iz $y > x$ slijedi $y \notin x$, dakle $\overline{x} \subset \overline{y}$, što je i trebalo dokazati.

Još moramo dokazati da inverz od $\overline{\cdot}$ čuva uređaj. No, prvo pitanje je: što je uopće inverz od $\overline{\cdot}$? Za svaki $y \in \overline{x}$ po (2.2) vrijedi $y \leqslant x$, što znači da je, po definiciji, x upravo najveći element od $\overline{x}$. Ovime smo pokazali da svaki $S \in \mathcal{A}$ ima najveći element — koji je očito jedinstven, pa ga označimo s $\max S$. Prirodno se nameće da ispitamo je li $g\colon \mathcal{A} \to A$, $g(S) := \max S$, inverz od $\overline{\cdot}$. Neka je $x \in A$. Tada je $g(\overline{x}) = \max \overline{x} = x$. Dakle, $g \circ \overline{\cdot} = \mathrm{id}$. Neka je sada $S \in \mathcal{A}$ i pretpostavimo $\max S = x$. Tada je $\overline{g(S)} = \overline{x}$. Da bismo dokazali da je $\overline{\cdot} \circ g = \mathrm{id}$, dovoljno je pokazati da je $S = \overline{x}$. Zato što je $S \in \mathcal{A}$, postoji $y \in A$ takav da je $S = \overline{y}$. No sada je $y = \max S$ po diskusiji od prije, te je $x = \max S$ po pretpostavci, dakle $x = y$, i onda $\overline{x} = \overline{y} = S$. Stoga je g uistinu inverz od $\overline{\cdot}$.

Pokažimo da g čuva uređaj. Neka su $S, T \in \mathcal{A}$ takvi da je $S \subset T$. Označimo $x := g(S)$ i $y := g(T)$. Iskoristimo li funkciju $\overline{\cdot}$ i činjenicu da je $\overline{\cdot} \circ g = \mathrm{id}$ dobivamo $S = \overline{x}$ i $T = \overline{y}$. Iz $S \subset T$ slijedi $\overline{x} \subset \overline{y}$. Kako je $x \in \overline{x}$, to je $x \in \overline{y}$, te, po definiciji $\overline{y}$, slijedi $x \leqslant y$. No, ne može biti $x = y$ jer bismo tada imali $\overline{x} = \overline{y}$, stoga je $x \neq y$. Dakle, $x < y$, što je i trebalo pokazati.

Izravno po definiciji zaključujemo da je $\overline{\cdot}$ sličnost između $(A, <)$ i $(\mathcal{A}, \subset)$ čime je dokaz gotov. □

Sljedeća Lema objedinjuje do sad izrečene rezultate i služi kao glavna motivacija za njihovo uvođenje.

Lema 2.2.11. *Ako tvrdnja Zornove leme vrijedi za parcijalno uređene skupove oblika* $\left(\{\overline{x} \mid x \in X\}, \subset\right)$, *gdje je* $(X, <)$ *parcijalno uređen skup i* $\overline{x} = \{y \in X \mid y \leqslant x\}$, *onda vrijedi za sve parcijalno uređene skupove.*

Dokaz. Neka je $(A, <)$ parcijalno uređen skup i $(\mathcal{A}, \subset)$ njemu sličan parcijalno uređen skup iz Leme 2.2.10. Neka je $f\colon \mathcal{A} \to A$ sličnost između $(\mathcal{A}, \subset)$ i $(A, <)$. Pretpostavimo da svaki lanac u A ima gornju među u A. Neka je $\mathcal{L}$ lanac u $\mathcal{A}$. Tada je po Propoziciji 2.2.7, tvrdnji 4) $f[\mathcal{L}]$ lanac u A. Po istoj Propoziciji, tvrdnji 3), i pretpostavci da $f[\mathcal{L}]$ ima gornju među u A zaključujemo da $\mathcal{L}$ ima gornju među u $\mathcal{A}$.

S obzirom da svaki lanac u $\mathcal{A}$ ima gornju među u $\mathcal{A}$, po pretpostavci ove Leme slijedi da $\mathcal{A}$ posjeduje maksimalni element. No, po Propoziciji 2.2.7, tvrdnji 1) sada slijedi i da A posjeduje maksimalni element. □

Zbog Leme 2.2.11 znamo da je dovoljno Zornovu lemu dokazati u nešto specijalnijem obliku.

Lema 2.2.12. *Neka je* $(\mathcal{S}, \subset)$ *parcijalno uređen skup sa svojstvom opisanim u Lemi 2.2.11 i neka svaki lanac u* $\mathcal{S}$ *ima gornju među u* $\mathcal{S}$. *Tada* $(\mathcal{S}, \subset)$ *ima barem jedan maksimalni element.*

2.3 Dokaz Zornove leme

Neka je $(\mathcal{S}, \subset)$ parcijalno uređen skup iz Leme 2.2.12. Označimo sa C skup svih lanaca u X (sjetimo se, $(X, <)$ je parcijalno uređen skup takav da je $\mathcal{S} = \{\overline{x} \mid x \in X\}$, gdje je, za $x \in X$, $\overline{x} = \{y \in X \mid y \leqslant x\}$). Proučavat ćemo parcijalno uređeni skup $(C, \subset)$ (što ima smisla jer su elementi od C podskupovi od X).

Tvrdnja 2.3.1. Vrijedi sljedeće:

a) Ako je $A \in C$, onda je i svaki podskup od A u C.

b) Ako je $\mathcal{L}$ lanac u C, onda je unija njegovih elemenata $L := \bigcup_{Y \in \mathcal{L}} Y$ u C.

c) Svaki lanac u C ima najmanju gornju među u C.

Dokaz. Kako je podskup svakog lanca očito lanac, tvrdnja a) očito vrijedi.

Da dokažemo tvrdnju b), trebamo dokazati da za sve $a, b \in L$ vrijedi $a < b$, $a = b$, ili $a > b$. Po definiciji od L tada postoje $Y_1, Y_2 \in \mathcal{L}$ takvi da je $a \in Y_1$ i $b \in Y_2$. Kako je $\mathcal{L}$ lanac, vrijedi ili $Y_1 \subseteq Y_2$ ili $Y_2 \subseteq Y_1$. Pretpostavimo da vrijedi $Y_1 \subseteq Y_2$ (drugi slučaj se dokazuje analogno). Tada su $a, b \in Y_2$. Kako je $\mathcal{L} \subseteq C$ i $Y_2 \in \mathcal{L}$, to je Y_2 lanac u X. Dakle, vrijedi ili $a < b$ ili $a = b$ ili $b < a$, što je i trebalo pokazati.

Za tvrdnju c), uz oznake iz tvrdnje b), uočimo da činjenica da je L lanac u X povlači da je $L \in C$. Očito je L gornja međa za $\mathcal{L}$. No, to je i najmanja gornja međa! Uistinu, ako je M neka druga gornja međa, vrijedi $M \supseteq Y$ za sve $Y \in \mathcal{L}$ pa je $M \supseteq \bigcup_{Y \in \mathcal{L}} Y = L$. □

Tvrdnja 2.3.2. Svaki element iz C sadržan u nekom elementu iz $\mathcal{S}$.

Dokaz. Neka je $L \in C$. Tada je L lanac u X pa je po Propoziciji 2.2.7, tvrdnji 4), $\overline{L}$ lanac u $\mathcal{S}$ (sjetimo se, $\bar{\cdot}$ je sličnost između $(X, <)$ i $(\mathcal{S}, \subset)$). Po pretpostavci, $\overline{L}$ ima gornju među u $\mathcal{S}$. Po Propoziciji 2.2.7, tvrdnji 3), L ima gornju među u X. Neka je ta gornja međa m. Tada za svaki $y \in L$ vrijedi $y \leqslant m$ pa je sigurno $L \subseteq \{y \in X \mid y \leqslant m\} = \overline{m}$. No, $\overline{m} \in \mathcal{S}$. □

Tvrdnja 2.3.3. Ako je L maksimalni element u C i m je gornja međa od L, tada je $\overline{m}$ maksimalni element u $\mathcal{S}$.

Dokaz. Pretpostavimo da $\overline{m}$ nije maksimalni element u $\mathcal{S}$, drugim riječima, pretpostavimo da postoji $Y \in \mathcal{S}$ takav da je $\overline{m} \subset Y$. Po definiciji skupa $\mathcal{S}$ zaključujemo da postoji $y \in X$ takav da je $Y = \overline{y}$. To znači da je $\overline{m} \subset \overline{y}$, tj. mora biti $m < y$. Drugim riječima, za sve $x \in L$ vrijedi $x \leqslant m < y$, tj. $L' := L \cup \{y\}$ je lanac u X. Dakle, $L' \in \mathcal{C}$. Također, $L \subset L'$. Međutim, L je maksimalni element u $\mathcal{C}$. Kontradikcija! Dakle, $\overline{m}$ je maksimalni element u $\mathcal{S}$. □

Iz prethodnih dviju tvrdnji zaključujemo da za svaki maksimalni element u $\mathcal{C}$ postoji odgovarajući maksimalni element u $\mathcal{S}$. Dakle, dovoljno je dokazati da $\mathcal{C}$ ima barem jedan maksimalni element.

Prema aksiomu izbora (Tvrdnja 1.3.3) postoji funkcija f koja svakom nepraznom podskupu S od X pridružuje element $f(S) \in S$. Za svaki $A \in \mathcal{C}$ označimo s $\tilde{A}$ skup svih $x \in X$ takvih da je $A \cup \{x\}$ lanac u X:

$$\tilde{A} := \{x \in X \mid A \cup \{x\} \in \mathcal{C}\}.$$

Definirajmo funkciju $g\colon \mathcal{C} \to \mathcal{C}$ s

$$g(A) := \begin{cases} A \cup \{f(\tilde{A} \setminus A)\}, & \text{ako } \tilde{A} \setminus A \neq \emptyset \\ A, & \text{ako } \tilde{A} \setminus A = \emptyset \end{cases}.$$

Napomena 2.3.4. Iz definicije od g je jasno da je $g(A) = A$ ako i samo ako je A maksimalni element od $\mathcal{C}$. Uistinu, ako je $g(A) = A$, onda je $\tilde{A} = A$ što znači da ne možemo dodati „nove” elemente u A, a da A i dalje ostane lanac. To upravo povlači da je A maksimalan u $\mathcal{C}$! S druge strane, ako $g(A) \neq A$, onda je $g(A) = A \cup \{f(\tilde{A} \setminus A)\} \supset A$ i, kako je $f(\tilde{A} \setminus A) \in \tilde{A}$, $g(A)$ je lanac. Dakle, A sigurno nije maksimalan u $\mathcal{C}$.

Definicija 2.3.5. Za $\mathcal{J} \subseteq \mathcal{C}$ kažemo da je g-*induktivan* ako vrijedi:

(i) $\emptyset \in \mathcal{J}$,

(ii) ako je $A \in \mathcal{J}$, onda je $g(A) \in \mathcal{J}$,

(iii) ako je $\mathcal{L} \subseteq \mathcal{J}$ lanac u $\mathcal{J}$, onda je $\bigcup_{J \in \mathcal{L}} J \in \mathcal{J}$.

Primijetimo najprije da je $\mathcal{C}$ g-induktivan. Dakle, g-induktivni skupovi postoje.

Tvrdnja 2.3.6. Neka je $(\mathcal{J}_i : i \in I)$ familija g-induktivnih skupova. Tada je $\mathcal{K} := \bigcap_{i \in I} \mathcal{J}_i$ g-induktivan.

Dokaz. Dokazujemo da $\mathcal{K}$ zadovoljava sva tri svojstva iz Definicije 2.3.5.

Svaki $\mathcal{J}_i$ je g-induktivan pa je $\emptyset \in \mathcal{J}_i$ za sve $i \in I$. Dakle, mora biti i $\emptyset \in \mathcal{K}$ pa je svojstvo (i) zadovoljeno.

Da bismo dokazali da je svojstvo (ii) zadovoljeno, pretpostavimo da je $A \in \mathcal{K}$. To znači da je $A \in \mathcal{J}_i$ za sve $i \in I$. Kako su svi $\mathcal{J}_i$ g-induktivni, slijedi da je $g(A) \in \mathcal{J}_i$ za sve $i \in I$. Iz definicije od $\mathcal{K}$ slijedi da je onda $g(A) \in \mathcal{K}$ pa je svojstvo (ii) zadovoljeno.

Neka je $\mathcal{L}$ lanac u $\mathcal{K}$. To je onda lanac i u $\mathcal{J}_i$ za sve $i \in I$. Svi $\mathcal{J}_i$ su g-induktivni pa je $\bigcup_{K \in \mathcal{L}} K \in \mathcal{J}_i$. No, to znači da je $\bigcup_{K \in \mathcal{L}} K \in \mathcal{K}$, stoga je svojstvo (iii) zadovoljeno. □

Označimo sa $\mathcal{K}_0$ presjek svih g-induktivnih skupova. Po upravno dokazanoj tvrdnji, $\mathcal{K}_0$ je g-induktivni skup. To je očito ujedno i najmanji g-induktivni skup. Dokažimo da je $\mathcal{K}_0$ lanac u C.

Neka je $C \in \mathcal{K}_0$ usporediv sa svim elementima od $\mathcal{K}_0$; drugim riječima, za sve $A \in \mathcal{K}_0$ vrijedi $C \subseteq A$ ili $A \subseteq C$. Uočimo da takvi elementi uistinu postoje, npr. $\emptyset$ je takav jer za sve $A \in \mathcal{K}_0$ imamo $\emptyset \subseteq A$. Nadalje, neka je $A \in \mathcal{K}_0$ pravi podskup od C. Kako je $g(A) \in \mathcal{K}_0$ po svojstvu (ii) i C usporediv sa svim elementima od $\mathcal{K}_0$, vrijedi ili $g(A) \subseteq C$ ili $C \subset g(A)$. No, drugi slučaj nije moguć — imali bismo $A \subset C \subset g(A)$, iz čega slijedi da $g(A)$ ima barem dva elemenata više od A, što je nemoguće po definiciji funkcije g (ili je $g(A) = A$ ili $g(A)$ ima točno jedan element više nego A). Dakle, za $C \in \mathcal{K}_0$ usporediv sa svim elementima iz $\mathcal{K}_0$, $\mathcal{K}_0 \ni A \subset C$ povlači $g(A) \subseteq C$.

Za svaki $C \in \mathcal{K}_0$ definiramo

$$I(C) := \{A \in \mathcal{K}_0 \mid A \subseteq C \text{ ili } g(C) \subseteq A\}.$$

Dokažimo da za sve $C \in \mathcal{K}_0$ vrijedi $I(C) = \mathcal{K}_0$. Inkluzija $I(C) \subseteq \mathcal{K}_0$ je očita iz definicije od $I(C)$. Kako je $\mathcal{K}_0$ najmanji g-induktivni skup, da bismo dokazali da je $\mathcal{K}_0 \subseteq I(C)$, dovoljno je dokazati da je $I(C)$ g-induktivan.

Tvrdnja 2.3.7. $I(C)$ je g-induktivan.

Dokaz. Sasvim je jasno da je $\emptyset \in I(C)$, pa $I(C)$ zadovoljava svojstvo (i). Neka je $A \in I(C)$. Dokazat ćemo da je tada i $g(A) \in I(C)$. Uočimo prvo da je $g(A) \in \mathcal{K}_0$ jer je $A \in I(C) \subseteq \mathcal{K}_0$ i za $\mathcal{K}_0$ vrijedi (ii). Mogu nastupiti dva slučaja. Ako je $A \subset C$, onda je $g(A) \subseteq C$, što odmah povlači da je $g(A) \in I(C)$. Ako je $A \supseteq g(C)$, onda je $g(A) \supseteq A \supseteq g(C)$ pa je opet $g(A) \in I(C)$. Dakle, $I(C)$ zadovoljava svojstvo (ii).

Dokažimo da zadovoljava i svojstvo (iii). Neka je $\mathcal{L}$ lanac u $I(C)$. Mogu nastupiti dva slučaja:

1. Za svaki $J \in \mathcal{L}$ je $J \subseteq C$. Jasno je da je $\bigcup_{J \in \mathcal{L}} J \subseteq C$. No, $\mathcal{K}_0$ zadovoljava svojstvo (iii) pa znamo i da je $\bigcup_{J \in \mathcal{L}} J \in \mathcal{K}_0$ (očito je $\mathcal{L}$ lanac u $\mathcal{K}_0$ jer je, sjetimo se, $I(C) \subseteq \mathcal{K}_0$). Dakle, mora biti $\bigcup_{J \in \mathcal{L}} J \in I(C)$.

2. Postoji $J_0 \in \mathcal{L}$ takav da je $J_0 \not\subseteq C$, tj. $g(C) \subseteq J_0$ pa je sigurno $g(C) \subseteq \bigcup_{J \in \mathcal{L}} J$. Kao i u prvom slučaju sada zaključujemo $\bigcup_{J \in \mathcal{L}} J \in I(C)$.

Dakle, $I(C)$ zadovoljava i svojstvo (iii) pa je g-induktivan. □

Znamo da je $I(C) \subseteq \mathcal{K}_0$, a iz upravo dokazane tvrdnje vrijedi i $\mathcal{K}_0 \subseteq I(C)$. Zaključujemo da je $I(C) = \mathcal{K}_0$.

Tvrdnja 2.3.8. $\mathcal{K}_0$ je lanac u C.

Dokaz. Neka je $C \in \mathcal{K}_0$ proizvoljan. Tada vrijedi $\mathcal{K}_0 = I(C)$. Drugim riječima, za sve $K \in \mathcal{K}_0$ vrijedi ili $K \subseteq C$ ili $g(C) \subseteq K$. U drugom slučaju vrijedi $C \subseteq K$. Dakle, C je usporediv sa svim elementima u $\mathcal{K}_0$. Međutim, zbog proizvoljnosti od C zaključujemo da su svaka dva elementa iz $\mathcal{K}_0$ usporediva. Dakle, $\mathcal{K}_0$ je uistinu lanac. □

Neka je $K_0 := \bigcup_{K \in \mathcal{K}_0} K$. Po svojstvu (iii) vrijedi da je $K_0 \in \mathcal{K}_0$. Kako $\mathcal{K}_0$ zadovoljava svojstvo (ii), imamo i da je $g(K_0) \in \mathcal{K}_0$. No, K_0 je unija svih elemenata iz $\mathcal{K}_0$ pa je $g(K_0) \subseteq K_0$. Međutim, znamo da vrijedi i $K_0 \subseteq g(K_0)$ pa je $K_0 = g(K_0)$. Po Napomeni 2.3.4 zaključujemo da je K_0 maksimalni element u C.

2.4 Primjeri korištenja Zornove leme

U ovoj sekciji izlažemo nekoliko primjera korištenja Zornove leme. Od čitatelja se očekuje osnovno znanje pojmova iz algebre, linearne algebre, teorije mjere i sličnog da bi mogao pratiti dokaze.

Kada imamo neprazni parcijalno uređen skup, nije potrebno promatrati sve lance, nego samo one neprazne, što ćemo sada dokazati.

Propozicija 2.4.1. Neka je $(A, <)$ neprazni parcijalno uređen skup koji ima svojstvo da svaki neprazni lanac u A ima gornju među u A. Tada $(A, <)$ ima barem jedan maksimalni element.

Dokaz. Neka je $\mathcal{L}$ lanac u A. Ako je $\mathcal{L} \neq \emptyset$, onda iz pretpostavke slijedi da $\mathcal{L}$ ima gornju među u A.

Pretpostavimo da je $\mathcal{L} = \emptyset$ (uočimo: $\emptyset$ je uvijek lanac u A). Kako je A neprazan, postoji neki element $a \in A$. Dodatno, trivijalno je a gornja međa od $\mathcal{L}$.

Dakle, svaki lanac u A ima gornju među u A, pa po Zornovoj lemi znamo da $(A, <)$ ima barem jedan maksimalni element, kao što se tvrdilo. □

Svaki vektorski prostor ima bazu

Neka je V vektorski prostor. Cilj nam je dokazati da ima bazu. U tu svrhu, definirajmo skup $\mathcal{S} := \{S \subseteq V \mid S \text{ linearno nezavisan}\}$. Dokazat ćemo da $\mathcal{S}$ ima $\subset$-maksimalni element.

Trivijalno je $\emptyset \subseteq V$ linearno nezavisan pa je $\emptyset \in \mathcal{S}$, tj. $\mathcal{S} \neq \emptyset$. Neka je $\mathcal{L}$ neprazni $\subset$-lanac u $\mathcal{S}$. Tvrdimo da je $U := \bigcup_{S \in \mathcal{L}} S$ gornja međa za $\mathcal{L}$ u odnosu na relaciju $\subset$ te da se U nalazi u $\mathcal{S}$. Za svaki $T \in \mathcal{L}$ vrijedi $T \subseteq \bigcup_{S \in \mathcal{L}} S = U$, dakle U je uistinu gornja međa od $\mathcal{L}$. Dokazat ćemo da je $U \in \mathcal{S}$, tj. da je U linearno nezavisan ($U \subseteq V$ vrijedi zato što je U unija skupova koji su svi podskupovi od V).

Najprije dokažimo jednu pomoćnu tvrdnju.

Tvrdnja 2.4.2. Skup $U \subseteq V$ je linearno nezavisan ako i samo ako mu je svaki konačni podskup linearno nezavisan.

Dokaz. Ako je U beskonačan, tvrdnja je upravo definicija linearne nezavisnosti beskonačnih skupova.

Neka je U konačan. Pretpostavimo da je linearno nezavisan i neka je $U' \subseteq U$. U' je uvijek konačan kao podskup konačnog skupa. Tada je U' linearno nezavisan kao podskup linearno nezavisnog skupa (uistinu, u prikaz nulvektora kao linearne kombinacije vektora iz U' dodamo sve vektore iz $U \setminus U'$ s koeficijentima jednakim nuli). Obratno, ako je svaki konačan podskup od U linearno nezavisan, onda je i U linearno nezavisan jer je U konačan i $U \subseteq U$. $\square$

Neka je U' konačni podskup od U. Ako je $U' = \emptyset$ trivijalno je linearno nezavisan. Pretpostavimo sada da $U' \neq \emptyset$ i označimo mu elemente s $v_1, v_2, \ldots, v_n$. Da bismo dokazali da je U' linearno nezavisan, promatramo jednadžbu

$$c_1 v_1 + c_2 v_2 + \cdots + c_n v_n = 0_V, \tag{2.3}$$

gdje su $c_1, c_2, \ldots, c_n$ skalari, a 0_V je nulvektor. Iz definicije skupa U znamo da postoje $S_1, S_2, \ldots, S_n \in \mathcal{L}$ takvi da $v_i \in S_i$ za $i = 1, 2, \ldots, n$. Dodatno, S_i, $i = 1, 2, \ldots, n$, su elementi lanca $\mathcal{L}$ pa je $\mathcal{X} := \{S_i \mid i = 1, 2, \ldots, n\}$ lanac u $\mathcal{S}$ kao podskup lanca. Po Propoziciji 2.1.12 znamo da ima $\mathcal{X}$ ima najveći element; označimo ga sa S_{i_0}. Dakle, $S_i \subseteq S_{i_0}$ za sve $i = 1, 2, \ldots, n$. Drugim riječima, imamo $v_1, v_2, \ldots, v_n \in S_{i_0}$. Sada se prisjetimo da je S_{i_0} linearno nezavisan pa iz jednadžbe (2.3) slijedi $c_1 = c_2 = \cdots = c_n = 0$. To upravo dokazuje da je U' linearno nezavisan!

Dokazali smo da je svaki konačni podskup od U linearno nezavisan pa po Tvrdnji 2.4.2 zaključujemo da je U linearno nezavisan. Drugim riječima, $U \in \mathcal{S}$.

Dokazali smo da svaki neprazni $\subset$-lanac u $\mathcal{S}$ ima gornju među u $\mathcal{S}$. Iz Propozicije 2.4.1 sada znamo da postoji $\subset$-maksimalan element od $\mathcal{S}$; fiksirajmo jedan maksimalni element i označimo ga s B. Ako B razapinje cijeli V, tada je B baza za V, pa smo gotovi. Pretpostavimo zato da B ne razapinje cijeli V. Tada postoji $v \in V$ koji nije linearna kombinacija konačno mnogo elemenata iz B. Specijalno, $v \notin B$. Promatrajmo skup $U_1 := B \cup \{v\}$. Očito je $B \subset U_1$. Također, $U_1 \subseteq V$.

Pokažimo da je U_1 linearno nezavisan. Neka je U_1' konačni podskup od U_1. Ako $v \notin U_1'$, onda je $U_1' \subseteq B$ pa je linearno nezavisan kao podskup linearno nezavisnog skupa. Ako je $U_1' = \{v\}$, onda je opet linearno nezavisan. Naime, uočimo da je $v \neq 0_V$ jer bi inače bio linearna kombinacija elemenata iz B; sada jednadžba $cv = 0_V$ za skalar c implicira $c = 0$. Ostaje ispitati slučaj kada je $U_1' = \{u_1, u_2, \ldots, u_n, v\}$ za neke $u_1, u_2, \ldots, u_n \in B$. Opet promatramo jednadžbu

$$c_1u_1 + c_2u_2 + \cdots + c_nu_n + cv = 0_V. \tag{2.4}$$

Uočimo da ako je $c \neq 0$ dobivamo

$$v = -\frac{c_1}{c}u_1 - \frac{c_2}{c}u_2 - \cdots - \frac{c_n}{c}u_n,$$

stoga je v linearna kombinacija elemenata iz B, što je kontradikcija. Dakle, mora biti $c = 0$. No onda se jednadžba (2.4) reducira u

$$c_1u_1 + c_2u_2 + \ldots + c_nu_n = 0_V,$$

te zbog linearne zavisnosti od B slijedi $c_1 = c_2 = \cdots = c_n = 0$. Dakle, dokazali smo da je U_1' linearno nezavisan.

Svaki konačni podskup od U_1 je linearno nezavisan pa je, po Tvrdnji 2.4.2, i U_1 linearno nezavisan. Međutim, sada imamo $B \subset U_1$ i $U_1 \in \mathcal{S}$, što je kontradikcija s činjenicom da je B upravo $\subset$-maksimalni element u $\mathcal{S}$. Drugim riječima, naša pretpostavka da B ne razapinje cijeli V je kriva, stoga je B baza za V. Ovime je dokaz gotov.

Teichmüller–Tukeyeva lema

U prethodnoj točki smo dokazali da svaki vektorski prostor ima bazu. Pritom smo koristili jedno svojstvo familije linearno nezavisnih podskupova vektorskog prostora, iskazano u Tvrdnji 2.4.2, koje se često pojavljuje i omogućuje jednostavniji dokaz egzistencije maksimalnog elementa nego direktna primjena Zornove leme.

Definicija 2.4.3. Za skup skupova $\mathcal{F}$ kažemo da je *konačne karakteristike* ako ima sljedeća svojstva:

(i) Za sve $A \in \mathcal{F}$, svaki konačni podskup od A je u $\mathcal{F}$.

(ii) Ako je A skup takav da je svaki njegov konačni podskup u $\mathcal{F}$, tada je $A \in \mathcal{F}$.

Tvrdnja 2.4.4 (Teichmüller–Tukeyeva lema)**.** Neka je Z skup i $\mathcal{F} \subseteq \mathcal{P}(Z)$. Ako je $\mathcal{F}$ konačne karakteristike i $X \in \mathcal{F}$, tada postoji $\subset$-maksimalni element od $\mathcal{F}$ koji sadrži X.

Dokaz. Definiramo
$$\mathcal{G} = \{Y \in \mathcal{F} \mid X \subseteq Y\}.$$
Uočimo da $\mathcal{G} \neq \emptyset$ jer je npr. $X \in \mathcal{G}$. Da bismo dokazali tvrdnju Teichmüller–Tukeyeve leme, pokazat ćemo da $\mathcal{G}$ posjeduje $\subset$-maksimalni element.

Neka je $\mathcal{L}$ neprazni lanac u $\mathcal{G}$. Definiramo $M := \bigcup_{Y \in \mathcal{L}} Y$. Tvrdimo da je M u $\mathcal{G}$. Za to ćemo iskoristiti svojstvo (ii). Dakle, uzmimo proizvoljni konačni podskup od M; označimo ga s M'. Označimo njegove elemente s $m_1, m_2, \ldots, m_n$. Po definiciji od M to znači da postoje $Y_1, Y_2, \ldots, Y_n \in \mathcal{L}$ takvi da je $m_i \in Y_i$ za sve $i = 1, 2, \ldots, n$.

Uočimo da je $\mathcal{X} := \{Y_i \mid i = 1, 2, \ldots, n\}$ lanac u $\mathcal{G}$ kao podskup lanca $\mathcal{L}$. Po Propoziciji 2.1.12 znamo da $\mathcal{X}$ ima najveći element; označimo ga s Y_{i_0}. Dakle, $Y_i \subseteq Y_{i_0}$ za sve $i = 1, 2, \ldots, n$ pa je $m_i \in Y_{i_0}$ za sve $i = 1, 2, \ldots, n$.

Za sada znamo da je $M' \subseteq Y_{i_0}$. No, $Y_{i_0} \in \mathcal{F}$ pa iz svojstva (i) zaključujemo da je $M' \in \mathcal{F}$.

Dokazali smo da je svaki konačni podskup od M u $\mathcal{F}$ pa iz svojstva (ii) slijedi da mora biti i $M \in \mathcal{F}$. Dodatno, za sve $Y \in \mathcal{L}$ vrijedi $Y \subseteq M$ pa je M gornja međa od $\mathcal{L}$ u $\mathcal{G}$. Po Propoziciji 2.4.1 sada slijedi da $\mathcal{G}$ posjeduje maksimalni element; fiksirajmo jedan maksimalni element i označimo ga s M_0.

Dokažimo da je M_0 maksimalan i u $\mathcal{F}$. Uistinu, ako nije, postoji neki $M_1 \in \mathcal{F}$ takav da $M_0 \subset M_1$. Dodatno, $X \subseteq M_0 \subset M_1$ pa je $M_1 \in \mathcal{G}$, što je kontradikcija s činjenicom da je M_0 $\subset$-maksimalni element od $\mathcal{G}$. □

Pogledajmo sad kako možemo jednostavnije dokazati tvrdnju iz prethodne točke.

Korolar 2.4.5. *Svaki vektorski prostor ima bazu.*

Dokaz. Neka je V vektorski prostor i neka je $\mathcal{F}$ skup linearno nezavisnih podskupova od V.

Neka je $A \in \mathcal{F}$ i neka je A' konačni podskup od A. Po Tvrdnji 2.4.2 zaključujemo da je $A' \in \mathcal{F}$. Ovime smo dokazali svojstvo (i) Definicije 2.4.3.

Da bismo dokazali i svojstvo (ii), uzmimo skup A takav da je svaki njegov konačni podskup u $\mathcal{F}$. Opet koristimo Tvrdnju 2.4.2 i zaključujemo da je $A \in \mathcal{F}$.

Po Tvrdnji 2.4.4 slijedi da postoji $\subset$-maksimalni element od $\mathcal{F}$ koji sadrži $\emptyset$ (jer je očito $\emptyset \in \mathcal{F}$); fiksirajmo jedan takav element i označimo ga s B. U prethodnoj točki smo pokazali da je svaki maksimalni element od $\mathcal{F}$ ujedno i baza za V pa je B baza za V. □

Svaki prsten s jedinicom ima maksimalni ideal

Neka je R prsten s jedinicom. Promatramo $\mathcal{S} := \{I \subset R \mid I \text{ je ideal u } R\}$. Dokazat ćemo da $\mathcal{S}$ ima $\subset$-maksimalni element. U tu svrhu, najprije uočimo da je $\{0\} \subset R$ ideal u R pa $\mathcal{S} \neq \emptyset$.

Neka je $\mathcal{L}$ neprazan $\subset$-lanac u $\mathcal{S}$. Definiramo $U := \bigcup_{S\in\mathcal{L}} S$. Očito za svaki $T \in \mathcal{L}$ vrijedi $T \subseteq \bigcup_{S\in\mathcal{L}} S = U$, tj. U je gornja međa od $\mathcal{L}$.

Dokažimo još da je $U \in \mathcal{S}$. Kada bi U bio cijeli R, specijalno bi vrijedilo $1 \in U$. Iz definicije od U slijedi da postoji $S \in \mathcal{L}$ takav da je $1 \in S$. Međutim, iz definicije ideala je jasno da bi tada vrijedilo da je $S = R$, što je kontradikcija s tim da je $S \in \mathcal{L} \subseteq \mathcal{S}$. Dakle, $1 \notin U$, iz čega zaključujemo i da $U \neq R$.

Dokažimo da je U ideal u R. Najprije, neka su $x, y \in U$. Po definiciji od U postoje $S_1, S_2 \in \mathcal{L}$ takvi da je $x \in S_1$ i $y \in S_2$. Mora vrijediti $S_1 \subseteq S_2$ ili $S_2 \subseteq S_1$. Ako je $S_1 \subseteq S_2$, onda imamo $x, y \in S_2$, te, kako je S_2 ideal u R, znamo i da je $x - y \in S_2$. Dakle, $x - y \in U$. Ako je $S_2 \subseteq S_1$, analogno zaključujemo da je $x - y \in U$. Slično zaključujemo i da je $xy \in U$. Dakle, U je potprsten od R.

Da bismo dokazali da je ideal, uzmimo $r \in R$ i $i \in U$. Po definiciji od U postoji $S \in \mathcal{L}$ takav da $i \in S$. Kako je S ideal u R, vrijedi $ir \in S$ i $ri \in S$. No, onda vrijedi i $ir \in U$ i $ri \in U$. Drugim riječima, U je ideal u R.

Svaki neprazni $\subset$-lanac u $\mathcal{S}$ ima gornju među u $\mathcal{S}$ pa iz Propozicije 2.4.1 slijedi da $\mathcal{S}$ ima maksimalni element; fiksirajmo jedan maksimalni element i označimo ga s M. Neka je I ideal u R za koji vrijedi $M \subset I \subseteq R$. Kada I ne bi bio cijeli R, imali bismo $I \in \mathcal{S}$, što je kontradikcija s maksimalnosti od M. Dakle, mora biti $I = R$, tj. dokazali smo da je M maksimalni ideal u R. Ovime je dokaz gotov.

Hartogsov teorem

Neka su A i B skupovi. Želimo pokazati da je ili $k(A) \leqslant k(B)$ ili $k(B) \leqslant k(A)$. Drugim riječima, ili postoji injekcija s A u B ili postoji injekcija s B u A. U tu svrhu, definiramo skup

$$\mathcal{F} := \{f\colon A' \to B' \mid f \text{ je injekcija, } A' \subseteq A,\ B' = \operatorname{Rng}(f) \subseteq B\}.$$

U nastavku dokaza koristit ćemo činjenicu da su funkcije relacije (preciznije, da je $\mathcal{F} \subseteq \mathcal{P}(A \times B)$) te ćemo tražiti $\subset$-maksimalni element od $\mathcal{F}$.

Uočimo da $\emptyset$ možemo shvatiti kao funkciju s $\emptyset$ u $\emptyset$ koja je trivijalno injekcija. Dakle, $\emptyset \in \mathcal{F}$ pa je $\mathcal{F} \neq \emptyset$. Neka je sada $\mathcal{L}$ neprazni $\subset$-lanac u $\mathcal{F}$ i definirajmo $g := \bigcup_{f\in\mathcal{L}} f$. Time smo očito dobili relaciju na $A \times B$, te vrijedi $h \subseteq \bigcup_{f\in\mathcal{L}} f = g$ za sve $h \in \mathcal{L}$. Pitanja na koja moramo odgovoriti u ostatku dokaza su: je li g funkcija kojoj je domena neki podskup od A, kojoj je slika neki podskup od B, i je li injekcija?

Pokazat ćemo da je g injektivna funkcija s domenom $D := \bigcup_{f\in\mathcal{L}} \operatorname{Dom}(f)$ i slikom $R := \bigcup_{f\in\mathcal{L}} \operatorname{Rng}(f)$. Pokažimo najprije da g ima funkcijsko svojstvo. Neka je $x \in D$. Po definiciji skupa D slijedi da postoji $f \in \mathcal{L}$ takva da $x \in \operatorname{Dom}(f)$. No, to znači da postoji jedinstveni $y \in \operatorname{Rng}(f)$ takav da je $(x, y) \in f$ (ili, drugačije zapisano, $f(x) = y$). Iz definicije od g je jasno da je $(x, y) \in g$. Također je jasno da je $y \in R$. Pretpostavimo sada da je $y' \in R$ takav da je $(x, y') \in g$. Po definiciji od g slijedi da postoji $h \in \mathcal{L}$ takva da je $(x, y') \in h$.

Kako je $\mathcal{L}$ $\subset$-lanac, vrijedi ili $h \subseteq f$ ili $f \subseteq h$. U prvom slučaju imamo da su (x, y') i (x, y) elementi od f. Međutim, f je funkcija, pa mora biti $y' = y$. Analogno zaključujemo u slučaju $f \subseteq h$. Dakle, za svaki $x \in D$ postoji jedinstveni $y \in R$ takav da je $(x, y) \in g$, tj. g je funkcija s D u R.

Pokažimo da je $\mathrm{Rng}(g) = R$. Očito je $\mathrm{Rng}(g) \subseteq R$. Neka je $y \in R$ proizvoljan. Po definiciji od R tada postoji $f \in \mathcal{L}$ takva da je $y \in \mathrm{Rng}(f)$. Nadalje, postoji $x \in \mathrm{Dom}(f)$ takav da je $(x, y) \in f$. Jasno, vrijedi i $(x, y) \in g$ te $x \in D$. Dakle, za svaki $y \in R$ postoji $x \in D$ takav da je $(x, y) \in g$ pa je $\mathrm{Rng}(g) = R$.

Pokažimo injektivnost. Neka je $y \in R$ i neka su $x, x' \in D$ takvi da su $(x, y), (x', y) \in g$. Po definiciji od g tada postoje $f_1, f_2 \in \mathcal{L}$ takve da je $(x, y) \in f_1$, $(x, y) \in f_2$. Kako je $\mathcal{L}$ $\subset$-lanac, vrijedi ili $f_1 \subseteq f_2$ ili $f_2 \subset f_1$. U prvom slučaju imamo $(x, y), (x', y) \in f_2$ što znači da mora biti $x = x'$ (sjetimo se, f_2 je injekcija). U drugom slučaju zaključujemo analogno. Dakle, g je injekcija.

Iz ovoga svega zaključujemo da je $g \in \mathcal{F}$. Dakle, svaki neprazni lanac u $\mathcal{F}$ ima gornju među u $\mathcal{F}$ pa iz Propozicije 2.4.1 slijedi da $\mathcal{F}$ ima $\subset$-maksimalni element; neka je $h\colon \tilde{A} \to \tilde{B} = \mathrm{Rng}(h)$ jedan maksimalni element u $(\mathcal{F}, \subset)$. Pokažimo da mora biti $\tilde{A} = A$ ili $\tilde{B} = B$. U suprotnom, postoje $a \in A \setminus \tilde{A}$ i $b \in B \setminus \tilde{B}$. Definirajmo $h_1\colon \tilde{A} \cup \{a\} \to \tilde{B} \cup \{b\}$ s

$$h_1(x) = \begin{cases} h(x), & x \neq a \\ b, & x = a \end{cases}.$$

Lako se vidi da je h_1 dobro definirana funkcija, da je $h_1 \in \mathcal{F}$, te da vrijedi $h \subset h_1$. Međutim, to je kontradikcija s činjenicom da je h $\subset$-maksimalni element od $\mathcal{F}$.

Ako je $\tilde{A} = A$, onda je h injekcija s A u B. Ako je $\tilde{B} = B$, onda je $h^{-1}\colon B \to \tilde{A}$ injekcija s B u A. Ovime je dokaz Hartogsovog teorema gotov.

Hausdorffov princip maksimalnosti

Dokazat ćemo ekvivalenciju Zornove leme i Hausdorffovog principa maksimalnosti.

Tvrdnja 2.4.6. Zornova lema povlači Hausdorffov princip maksimalnosti.

Dokaz. Neka je $(A, <)$ parcijalno uređen skup. Tvrdimo da je svaki lanac u A podskup nekog maksimalnog lanca. Neka je L proizvoljni lanac u A. Definiramo skup

$$C_L := \{K \subseteq A \mid L \subseteq K \text{ i } K \text{ je lanac u } A\}$$

i parcijalno ga uredimo relacijom $\subset$.

Očito $C_L \neq \emptyset$ jer je recimo $L \in C$. Neka je $\mathcal{L}$ neprazni $\subset$-lanac u C_L i definiramo $M := \bigcup_{K \in \mathcal{L}} K$. Tvrdimo da je $M \in C_L$, tj. da je $L \subseteq M$ i da je M lanac u A. Očito je da je

$L \subseteq M$ jer su svi $K \in \mathcal{L}$ nadskupovi od L. Po Tvrdnji 2.3.1 b) znamo i da je M lanac u A. Dodatno, očito je $K \subseteq M$ za sve $K \in \mathcal{L}$.

Dakle, svaki lanac u C_L ima gornju među u C_L pa po Propoziciji 2.4.1 slijedi da C_L ima maksimalni element; fiksirajmo jedan maksimalni element i označimo ga s K_0. Uočimo da je $L \subseteq K_0$.

Tvrdimo da je K_0 maksimalni lanac u A. Doista, ako je K_1 lanac u A takav da je $K_0 \subset K_1$, onda specijalno vrijedi i $L \subseteq K_1$ pa je $K_1 \in C_L$, što je kontradikcija s maksimalnosti od K_0 (u C_L). Drugim riječima, K_0 je maksimalni lanac u A. Ovime je dokaz gotov. □

Tvrdnja 2.4.7. Hausdorffov princip maksimalnosti povlači Zornovu lemu.

Dokaz. Neka je $(A, <)$ parcijalno uređen skup takav da svaki lanac u A ima gornju među u A. Pretpostavimo da A ne posjeduje maksimalni element. $\emptyset$ je lanac u A pa je po Hausdorffovom principu maksimalnosti podskup nekog maksimalnog lanca; jedan takav označimo s M.

Neka je m neka njegova gornja međa u A (koja postoji po pretpostavci Zornove leme). Dakle, za sve $x \in M$ vrijedi $x \leqslant m$. Kako A ne posjeduje maksimalni element, to m nije maksimalni element od A, stoga postoji neki $n \in A$ takav da je $m < n$. Kako je m gornja međa od M, a $m < n$, znamo da $n \notin M$. Zbog tranzitivnosti od $<$ za sve $x \in M$ vrijedi $x < n$. Iz ovoga slijedi da je $M \cup \{n\}$ lanac u A. No, znamo i da je $M \subset M \cup \{n\}$ (jer $n \notin M$). Ovo je kontradikcija s činjenicom da je M maksimalni lanac u A.

Dakle, pretpostavka da A nema maksimalni element je bila kriva, tj. A posjeduje barem jedan maksimalni element. □

Lanac skupova mjere nula

Promatramo $\mathbb{R}$ i Lebesgueovu mjeru λ. Skup $A \subseteq R$ zovemo *nul-skup* ako je $\lambda(A) = 0$. Dokazat ćemo da postoji lanac nul-skupova takav da unija elemenata tog lanca nije nul-skup. Uistinu, pretpostavimo suprotno, tj. da takav lanac ne postoji, i pokušat ćemo doći do kontradikcije.

Definiramo skup

$$\mathcal{M}_0 := \{S \subseteq \mathbb{R} \mid \lambda(S) = 0\}$$

i parcijalno ga uredimo relacijom $\subset$. Očito $\mathcal{M}_0 \neq \emptyset$ jer je npr. $\emptyset \in \mathcal{M}_0$. Neka je $\mathcal{L}$ proizvoljni neprazni lanac u $\mathcal{M}_0$. Definiramo $M := \bigcup_{L \in \mathcal{L}} L$. Vrijedi $\lambda(M) = 0$ (po pretpostavci koju smo uveli) pa je $M \in \mathcal{M}_0$. Dodatno, M je gornja međa od $\mathcal{L}$ u $\mathcal{M}_0$.

Po Propoziciji 2.4.1 slijedi da $\mathcal{M}_0$ ima maksimalni element; fiksirajmo jedan maksimalni element i označimo ga s M_0. Dodatno, $M_0 \neq \mathbb{R}$ jer $\lambda(\mathbb{R}) \neq 0$. To znači da postoji neki $x \in \mathbb{R} \setminus M_0$. Vrijedi

$$\lambda(M_0 \cup \{x\}) = \lambda(M_0) + \lambda(\{x_0\}) = 0 + 0 = 0,$$

gdje prva jednakost slijedi iz disjunktnosti od M_0 i $\{x\}$, a druga jednakost slijedi iz činjenice da su jednočlani skupovi mjere nula.

Dakle, $M_0 \cup \{x\} \in \mathcal{M}_0$. No, $M_0 \subset M_0 \cup \{x\}$, što je kontradikcija s činjenicom da je M_0 maksimalan u $\mathcal{M}_0$. S obzirom da smo došli do kontradikcije, zaključujemo da mora postojati lanac nul-skupova takav da unija elemenata tog lanca nije nul-skup.

Poglavlje 3

Zermelov teorem

3.1 Uvodno o Zermelovom teoremu

Zermelov teorem o dobrom uređaju je još jedan važan teorem teorije skupova. Najprije moramo odgovoriti što je to uopće dobar uređaj.

Definicija 3.1.1. Za parcijalno uređeni skup $(A, <)$ kažemo da je *dobro uređen*, odnosno da je $<$ *dobar uređaj* na A, ako svaki neprazni podskup od A sadrži najmanji element.

Vjerojatno najpoznatiji primjer dobro uređenog skupa je $(\mathbb{N}, <)$, gdje $<$ označava standardni uređaj na $\mathbb{N}$. Također, lako se pokaže da na svakom konačnom skupu S možemo naći dobar uređaj. Prirodno pitanje koje sad možemo postaviti je: na kojim sve skupovima postoje dobri uređaji? To pitanje još možemo izreći kao: koji se sve skupovi mogu *dobro urediti*? Pokazuje se da, ako pretpostavimo aksiom izbora, možemo dobro urediti *svaki* skup!

Teorem 3.1.2 (Zermelov teorem o dobrom uređaju)**.** *Svaki skup se može dobro urediti, tj. za svaki skup A postoji relacija $R \subseteq A \times A$ takva da je (A, R) dobro uređen skup.*

Napomena 3.1.3. Uočimo da se, korištenjem Teorema 3.1.2, $\mathbb{R}$ može dobro urediti. Neka je $\prec$ dobar uređaj na $\mathbb{R}$. Kako ga karakterizirati? Točnije, kako zapisati nekim preciznim uvjetom na $x, y \in \mathbb{R}$ kada vrijedi $x \prec y$? Problem je u tome što ne znamo. Kao što smo već nekoliko puta spomenuli, aksiom izbora nije konstruktivan. To isto vrijedi i za Zermelov teorem o dobrom uređaju (jer mu je ekvivalentan).

Jedna povijesna zanimljivost je da je Cantor smatrao da je „razumno" pretpostaviti da se svaki skup može dobro urediti. No, kao što smo istaknuli u Napomeni 3.1.3, već kod često korištenih skupova se pojavljuje problem da je jako teško, a možda čak i nemoguće, precizno opisati taj dobar uređaj.

Dokaz Teorema 3.1.2 provodimo uporabom Zornove leme. Promatrat ćemo $\mathcal{F}$ kao (neformalno govoreći) skup svih podskupova od A koji se mogu dobro urediti. Međutim, standardni pristup (unija $\subset$-lanca kao gornja međa) ovdje neće proći, o čemu govori sljedeća Napomena.

Napomena 3.1.4. Unija dobro uređenih skupova koji su u $\subset$-lancu ne mora biti dobro uređen skup. Uistinu, za $m \in \mathbb{Z}$ označimo $\mathbb{Z}_m := \{n \in \mathbb{Z} \mid n \geqslant m\}$. Tada je, za svaki $m \in \mathbb{Z}$, $(\mathbb{Z}_m, <)$ dobro uređen skup te je $\mathcal{L} = \{(\mathbb{Z}_m, <) \mid m \in \mathbb{Z}\}$ $\subset$-lanac dobro uređenih skupova. No, unija elemenata tog lanca je $(\mathbb{Z}, <)$, što nije dobro uređen skup.

Dakle, moramo $\mathcal{F}$ urediti nekom drugom relacijom. Naravno, prije uvođenja relacije, potrebno je i precizno definirati $\mathcal{F}$.

Definicija 3.1.5. Neka je A skup. Na skupu

$$\mathcal{F} := \{(S, R) \mid S \subseteq A \text{ i } (S, R) \text{ je dobro uređen skup}\}$$

definiramo relaciju

$$(S, R) \prec (T, Q) :\Leftrightarrow R = Q \cap (S \times S) \land (\exists y \in T)(S = \{x \in T \mid x\ Q\ y\}). \tag{3.1}$$

Ako vrijedi $(S, R) \prec (T, Q)$, kažemo još i da je (S, R) *početni komad od* (T, Q).

Napomena 3.1.6. Uočimo da je $\mathcal{F}$ zaista skup. Naime, možemo ga shvatiti kao relaciju između $\mathcal{P}(A)$ i $\mathcal{P}(A \times A)$ jer za $S \subseteq A$ i $R \subseteq A \times A$ vrijedi

$$(S, R) \in \mathcal{F} \Leftrightarrow (S, R) \text{ je dobro uređen skup.}$$

Lema 3.1.7. *Relacija $\prec$ zadana s* (3.1) *je relacija parcijalnog uređaja (na skupu $\mathcal{F}$).*

Dokaz. Najprije uočimo sljedeće: ako je $(S, R) \prec (T, Q)$, onda je $S \subset T$. Doista, iz definicije je jasno da je $S \subseteq T$. Dodatno, za y iz (3.1), zbog irefleksivnosti relacije Q, vrijedi $y \notin S$. Dakle, $S \neq T$.

Moramo dokazati irefleksivnost i tranzitivnost relacije $\prec$.

Neka je $(S, R) \in \mathcal{F}$. Kako je $S \not\subset S$, vrijedi i $(S, R) \not\prec (S, R)$. Drugim riječima, $\prec$ je irefleksivna relacija.

Neka su sada (S, R), (T, Q) i (U, P) dobro uređeni skupovi takvi da je (S, R) početni komad od (T, Q), koji je početni komad od (U, P). Željeli bismo dokazati da je (S, R) početni komad od (U, P). Najprije, uočimo da vrijedi $S \subseteq T \subseteq U$, $R = Q \cap (S \times S)$ i $Q = P \cap (T \times T)$ pa je $R = P \cap (S \times S)$. Dakle, vrijedi prvi uvjet u (3.1).

Dokažimo i drugi uvjet. Postoje $y_1 \in T$ i $y_2 \in U$ takvi da je $S = \{x \in T \mid x\ Q\ y_1\}$ i $T = \{x \in U \mid x\ P\ y_2\}$. Tvrdimo da je $S = \{x \in U \mid x\ P\ y_1\}$.

Neka je $x_0 \in S$. Vrijedi $S \subset T \subset U$ pa je $x_0 \in U$. Nadalje, $x_0\ Q\ y_1$ i $Q = P \cap (T \times T)$ povlači $x_0\ P\ y_1$. Dakle, $x_0 \in \{x \in U \mid x\ P\ y_1\}$, tj. $S \subseteq \{x \in U \mid x\ P\ y_1\}$.

Neka je $x_0 \in \{x \in U \mid x\ P\ y_1\}$. Tvrdimo da je $x_0 \in S$. Kako je $y_1 \in T$, to je $y_1\ P\ y_2$. Dakle, $x_0\ P\ y_2$. Kako je $x \in U$ i $x_0\ P\ y_2$, slijedi $x_0 \in T$. Za sada znamo da je $x_0 \in T$ i da vrijedi $x_0\ P\ y_1$. Zato što je Q dobar uređaj na T, vrijedi da je ili $x_0\ Q\ y_1$ ili $y_1\ Q\ x_0$. (Uočimo da je $x_0 = y_1$ nemoguće jer bismo inače imali $y_1\ P\ y_1$ što je kontradikcija s irefleksivnosti relacije P.) No, iz $y_1\ Q\ x_0$ slijedi $y_1\ P\ x_0$ (jer je $Q \subset P$), a iz tranzitivnosti relacije P slijedi i $y_1\ P\ y_1$. Ovo je kontradikcija s irefleksivnosti relacije P. Dakle, mora vrijediti $x_0\ Q\ y_1$ pa je $x_0 \in \{x \in T \mid x\ Q\ y_1\} = S$.

Konačno, zaključujemo da je $(S, R) \prec (U, P)$, tj. relacija $\prec$ je tranzitivna.

Relacija $\prec$ je irefleksivna i tranzitivna pa je relacija parcijalnog uređaja. □

Napomena 3.1.8. Uočimo da ako vrijedi $(A, R) \preccurlyeq (B, Q)$, onda je $R = Q \cap (A \times A)$. Za $(A, R) \prec (B, Q)$ to slijedi direktno iz (3.1), a za $(A, R) = (B, Q)$ tvrdnja slijedi zato što je $Q = R$ i $R \subseteq A \times A$, pa $Q \cap (A \times A) = R \cap (A \times A) = R$.

3.2 Dokaz Zermelovog teorema

Neka je A skup. Promatramo skup $\mathcal{F}$ i relaciju $\prec$ iz Definicije 3.1.5. Iz Leme 3.1.7 znamo da je $\prec$ relacija parcijalnog uređaja. Očito $\mathcal{F} \neq \emptyset$; na primjer, $(\emptyset, \emptyset) \in \mathcal{F}$.

Neka je $\mathcal{L} = \{(S_i, R_i) \mid i \in I\}$ neprazan lanac u $\mathcal{F}$. Definiramo $\mathcal{U} := (S, R)$, gdje su $S := \bigcup_{i \in I} S_i$ i $R := \bigcup_{i \in I} R_i$. Tvrdimo da je to gornja međa od $\mathcal{L}$ u $\mathcal{F}$.

Tvrdnja 3.2.1. Uz upravo uvedene oznake, $\mathcal{U}$ je linearno uređen skup.

Dokaz. Dokazujemo irefleksivnost, tranzitivnost, i linearnost relacije R na $S \times S$.

Da bismo dokazali irefleksivnost, pretpostavimo da postoji $x \in S$ takav da je $x\ R\ x$. Drugačije zapisano, to znači da je $(x, x) \in R$. Dakle, postoji $i_0 \in I$ takav da je $(x, x) \in R_{i_0}$. No, to znači da vrijedi $x\ R_{i_0}\ x$, tj. R_{i_0} nije irefleksivna. Kontradikcija! Dakle, za svaki $x \in S$ je $x \not R\ x$ pa je R irefleksivna relacija.

Da bismo dokazali tranzitivnost, pretpostavimo da su $x, y, z \in S$ takvi da $x\ R\ y$ i $y\ R\ z$. Po definiciji R zaključujemo da postoje $i_0, j_0 \in I$ takvi da $x\ R_{i_0}\ y$ i $y\ R_{j_0}\ z$. Kako je $\mathcal{L}$ lanac, imamo dvije mogućnosti: $(S_{i_0}, R_{i_0}) \preccurlyeq (S_{j_0}, R_{j_0})$ ili $(S_{j_0}, R_{j_0}) \prec (S_{i_0}, R_{i_0})$.

Ako je $(S_{i_0}, R_{i_0}) \preccurlyeq (S_{j_0}, R_{j_0})$, tada je $R_{i_0} = R_{j_0} \cap (S_{i_0} \times S_{i_0}) \subseteq R_{j_0}$, pa mora biti $x\ R_{j_0}\ y$. Iz tranzitivnosti relacije R_{j_0} slijedi $x\ R_{j_0}\ z$, a iz toga i $x\ R\ z$. Slučaj $(S_{j_0}, R_{j_0}) \prec (S_{i_0}, R_{i_0})$ se dokazuje analogno.

Pokazali smo da je R tranzitivna. Pokažimo sada linearnost. Neka su $x, y \in S$, $x \neq y$. Kako je $S = \bigcup_{i \in I} S_i$, zaključujemo da postoje $i_0, j_0 \in I$ takvi da $x \in S_{i_0}$ i $y \in S_{j_0}$. Opet imamo dvije mogućnosti: $(S_{i_0}, R_{i_0}) \preccurlyeq (S_{j_0}, R_{j_0})$ ili $(S_{j_0}, R_{j_0}) \prec (S_{i_0}, R_{i_0})$.

Ako je $(S_{i_0}, R_{i_0}) \preccurlyeq (S_{j_0}, R_{j_0})$, tada je $S_{i_0} \subseteq S_{j_0}$ pa je $x \in S_{j_0}$. Kako je (S_{j_0}, R_{j_0}) linearno uređen, slijedi $x\ R_{j_0}\ y$ ili $y\ R_{j_0}\ x$. Iz toga odmah slijedi da vrijedi $x\ R\ y$ ili $y\ R\ x$. Slučaj $(S_{j_0}, R_{j_0}) \prec (S_{i_0}, R_{i_0})$ se dokazuje analogno.

Dakle, $\mathcal{U}$ je linearno uređen skup. $\square$

Tvrdnja 3.2.2. $\mathcal{U}$ je dobro uređen skup.

Dokaz. Neka je Y proizvoljni neprazni podskup od S. Tvrdimo da ima R-najmanji element.

Najprije uočimo da iz $Y \subseteq S$ i $Y \neq \emptyset$ slijedi da postoji $i_0 \in I$ takav da $Y \cap S_{i_0} \neq \emptyset$. Dodatno, $Y \cap S_{i_0}$ je neprazni podskup od S_{i_0}. Kako je (S_{i_0}, R_{i_0}) dobro uređen skup slijedi da postoji $y \in Y \cap S_{i_0}$ koji je R_{i_0}-najmanji element u $Y \cap S_{i_0}$. Cilj nam je dokazati da je to R-najmanji element u Y.

Neka je $z \in Y$ takav da $z \neq y$. Slično kao i za y, postoji $i \in I$ takav da je $z \in Y \cap S_i$. Opet imamo dvije mogućnosti: $(S_i, R_i) \preccurlyeq (S_{i_0}, R_{i_0})$ ili $(S_{i_0}, R_{i_0}) \prec (S_i, R_i)$.

Ako je $(S_i, R_i) \preccurlyeq (S_{i_0}, R_{i_0})$, tada je $S_i \subseteq S_{i_0}$. To ujedno znači da je $z \in S_{i_0}$ te $z \in Y \cap S_{i_0}$. Dakle, kako je y upravo R_{i_0}-najmanji element u $Y \cap S_{i_0}$, mora biti $y\ R_{i_0}\ z$ te, zbog definicije od R, i $y\ R\ z$.

Neka je $(S_{i_0}, R_{i_0}) \prec (S_i, R_i)$. Kako je R_i linearni uređaj i $z \neq y$, vrijedi $y\ R_i\ z$ ili $z\ R_i\ y$. Pretpostavimo da je $z\ R_i\ y$. Po definiciji relacije $\prec$ i tranzitivnosti od R_i slijedi da je $z \in S_{i_0}$, te $z \in Y \cap S_{i_0}$. Kao i prije zaključujemo da je $y\ R_{i_0}\ z$. No, iz $(S_{i_0}, R_{i_0}) \prec (S_i, R_i)$ slijedi $R_{i_0} \subseteq R_i$ pa je $y\ R_i\ z$. Dakle, $y\ R_i\ z$ i $z\ R_i\ y$ pa, zbog tranzitivnosti relacije R_i, slijedi i $y\ R_i\ y$, što je nemoguće jer je R_i irefleksivna relacija! Pretpostavili smo da je $z\ R_i\ y$ iz čega smo dobili kontradikciju pa mora biti $y\ R_i\ z$. Iz definicije relacije R slijedi i $y\ R\ z$.

Rezimirajmo: za svaki $z \in Y$, $z \neq y$, vrijedi $y\ R\ z$. To upravo znači da je y R-najmanji element u Y. Dakle, Y ima R-najmanji element. Ujedno je Y bio proizvoljni neprazni podskup od S pa je $\mathcal{U}$ dobro uređen skup. $\square$

Tvrdnja 3.2.2 pokazuje da je $\mathcal{U} \in \mathcal{F}$.

Tvrdnja 3.2.3. $\mathcal{U}$ je gornja međa od $\mathcal{L}$.

Dokaz. Uzmimo proizvoljni $(S_i, R_i) \in \mathcal{L}$. Ako je $S = S_i$, iz linearnosti dobrih uređaja i $R_i \subseteq R$ lako slijedi da mora biti i $R = R_i$, pa je $(S_i, R_i) = (S, R)$.

Pretpostavimo zato da je $S \neq S_i$, odnosno $S_i \subset S$. Dokažimo da je $R \cap (S_i \times S_i) = R_i$.

Neka je $(x, y) \in R \cap (S_i \times S_i)$. Tada su $x, y \in S_i$ i vrijedi $x\ R\ y$. Kako je R_i dobar uređaj vrijedi ili $x\ R_i\ y$ ili $y\ R_i\ x$. No, iz $y\ R_i\ x$ bi slijedilo $y\ R\ x$ pa i $y\ R\ y$ (jer je R tranzitivna relacija), a to je kontradikcija s irefleksivnosti od R. Dakle, mora biti $x\ R_i\ y$, tj. $(x, y) \in R_i$.

Obratno, neka je $(x, y) \in R_i$. Izravno po definiciji od R slijedi $(x, y) \in R$. No, $x, y \in S_i$ (jer je R_i relacija na S_i) pa je ujedno $(x, y) \in R \cap (S_i \times S_i)$.

Dakle, vrijedi $R_i = R \cap (S_i \times S_i)$. Da dokažemo drugo svojstvo u (3.1), promatramo $S' := S \setminus S_i$. To je neprazan podskup od S pa ima R-najmanji element; označimo ga sa s. Dokazujemo da vrijedi $S_i = \{x \in S \mid x\ R\ s\}$.

Neka je $s_i \in S_i$ proizvoljan. Kako je R linearan, vrijedi ili $s_i\ R\ s$ ili $s\ R\ s_i$. Pretpostavimo da vrijedi $s\ R\ s_i$. Po definiciji od S slijedi da postoji $S_j \in \mathcal{L}$ takav da je $s \in S_j$. Kako je $\mathcal{L}$ lanac, vrijedi ili $(S_i, R_i) \prec (S_j, R_j)$ ili $(S_j, R_j) \prec (S_i, R_i)$ (uočimo da je, zbog $s \notin S_i$, $S_i \neq S_j$).

Pretpostavimo da je $(S_i, R_i) \prec (S_j, R_j)$. Po definiciji relacije $\prec$ postoji $y \in S_j$ takav da je $S_i = \{x \in S_j \mid x\ R_j\ y\}$. Zbog $s_i \in S_i$ vrijedi $s_i\ R_j\ y$. Dodatno, $s_i \in S_j$. Kako je R_j dobar uređaj, vrijedi ili $s_i\ R_j\ s$ ili $s\ R_j\ s_i$. No, prvi slučaj je nemoguć, jer implicira da je $s_i\ R\ s$ što, zbog $s\ R\ s_i$, implicira $s_i\ R\ s_i$, a to je kontradikcija s irefleksivnosti od R. Dakle, $s\ R_j\ s_i$. Iz tranzitivnosti od R_j slijedi i $s\ R_j\ y$. No, ovo implicira da je $s \in S_i$ (jer je $S_i = \{x \in S_j \mid x\ R_j\ y\}$), što je kontradikcija s izborom od s.

Pretpostavimo da je $(S_j, R_j) \prec (S_i, R_i)$. Tada vrijedi $S_j \subseteq S_i$, što znači da je $s \in S_i$, što je opet kontradikcija s izborom od s.

Pretpostavka da je $s\ R\ s_i$ vodi do kontradikcije, stoga je $s_i\ R\ s$. Ovime smo pokazali da je $S_i \subseteq \{x \in S \mid x\ R\ s\}$.

Obratno, neka je $x \in S$ takav da je $x\ R\ s$. Ako $x \notin S_i$, onda je $x \in S'$, a to je kontradikcija s činjenicom da je s R-najmanji element u S'. Dakle, $x \in S_i$, pa zbog proizvoljnosti od x slijedi $\{x \in S \mid x\ R\ s\} \subseteq S_i$.

Ovime smo pokazali $S_i = \{x \in S \mid x\ R\ s\}$, pa je $(S_i, R_i) \prec (S, R)$, što smo i htjeli pokazati. □

Po Propoziciji 2.4.1 slijedi da postoji maksimalni element od $\mathcal{F}$. Fiksirajmo jedan maksimalni element i označimo ga sa (S_0, R_0).

Tvrdnja 3.2.4. Vrijedi $S_0 = A$.

Dokaz. Po definiciji skupa $\mathcal{F}$ je $S_0 \subseteq A$. Pretpostavimo, suprotno Tvrdnji, da je $S_0 \subset A$. Tada postoji $a_1 \in A \setminus S_0$. Definirajmo $S_1 := S_0 \cup \{a_1\}$ i $R_1 := R_0 \cup \{(a, a_1) \mid a \in S_0\}$ (intuitivno, svi „stari” elementi su „manji” od „novoga”). Tvrdimo da je $\mathcal{U}_1 := (S_1, R_1)$ dobro uređen skup, tj. $\mathcal{U}_1 \in \mathcal{F}$.

Neka je $s \in S_1$. Ako je $s = a_1$, onda, zbog $a_1 \notin S_0$, vrijedi $s\ \not R_1\ s$. Ako je $s \neq a_1$, onda je $s \in S_0$ pa, zbog irefleksivnosti od R_0, vrijedi $s\ \not R_0\ s$. Iz toga slijedi i $s\ \not R_1\ s$. Konačno, zaključujemo da za sve $s \in S_1$ vrijedi $s\ \not R_1\ s$, tj. R_1 je irefleksivna relacija.

Neka su $x, y, z \in S_1$ takvi da $x\ R_1\ y$ i $y\ R_1\ z$. Ako su $x, y, z \in S_0$, iz definicije od R_1 znamo da je $x\ R_0\ y$ i $y\ R_0\ z$. Iz tranzitivnosti relacije R_0 zaključujemo da vrijedi $x\ R_0\ z$ pa onda i $x\ R_1\ z$. Pretpostavimo sada da ne vrijedi $x, y, z \in S_0$, tj. jedan od njih mora biti upravo a_1. Ako je $x = a_1$ onda je $x\ R_1\ y$ nemoguće. Slično slijedi i za $y = a_1$: tada je $y\ R_1\ z$ nemoguće. Dakle, mora biti $z = a_1$. No onda je $x\ R_1\ z$ trivijalno po definiciji R_1! Dakle, R_1 je tranzitivna relacija.

Neka su $x, y \in S_1$, $x \neq y$. Ako su $x, y \in S_0$, onda je $x\ R_0\ y$ ili $y\ R_0\ x$ po linearnosti od R_0. Iz ovoga slijedi da vrijedi ili $x\ R_1\ y$ (ako $x\ R_0\ y$) ili $y\ R_1\ x$ (ako $y\ R_0\ x$). Ako je $x = a_1$, onda izravno iz definicije od R_1 slijedi $y\ R_1\ x$. Ako je pak $y = a_1$, onda izravno iz definicije od R_1 slijedi $x\ R_1\ y$. Dakle, R_1 je linearni uređaj.

Neka je $Y \subseteq S_1$, $Y \neq \emptyset$. Ako je $Y \subseteq S_0$, onda ima R_0-najmanji element; označimo ga s y_0. Zbog definicije od R_1 vrijedi i $y_0\ R_1\ y$ za sve $y \in Y \setminus \{y_0\}$ pa je y_0 ujedno i R_1-najmanji element od Y.

S druge strane, ako je $a_1 \in Y$, onda definiramo $Y' := Y \setminus \{a_1\}$. Ako je $Y' \neq \emptyset$, po prethodno dokazanom Y' ima R_1-najmanji element; označimo ga s y. No ujedno vrijedi i $y\ R_1\ a_1$ po definiciji od R_1. Dakle, y je R_1-najmanji element od Y. Ako je pak $Y' = \emptyset$ onda je $Y = \{a_1\}$ pa je a_1 trivijalno R_1-najmanji element od Y.

Ovime smo dokazali da je R_1 dobar uređaj, tj. da je (S_1, R_1) dobro uređen skup. To znači da je $(S_1, R_1) \in \mathcal{F}$. No, $R_0 = R_1 \cap (S_0 \times S_0)$ i $S_0 = \{x \in S_1 \mid x\ R_1\ a_1\}$ pa je $(S_0, R_0) \prec (S_1, R_1)$, što je kontradikcija s maksimalnosti od (S_0, R_0). Zaključujemo da mora biti $S_0 = A$. $\square$

Iz $(S_0, R_0) = (A, R_0)$ zaključujemo da je R_0 dobar uređaj na A. Ovime je dokaz Zermelovog teorema gotov.

3.3 Zermelov teorem povlači aksiom izbora

Cilj nam je dokazati da tvrdnja Teorema 3.1.2 povlači tvrdnju Aksioma 0.0.2. Time ćemo dokazati „trokut implikacija”:

$$
\begin{tikzcd}
 & \boxed{\text{Zornova lema}} \arrow[dr, Rightarrow] & \\
\boxed{\text{Aksiom izbora}} \arrow[ur, Rightarrow] & & \boxed{\text{Zermelov teorem}} \arrow[ll, Rightarrow]
\end{tikzcd}
$$

Dakle, dokazat ćemo da su te tri tvrdnje međusobno ekvivalentne.

Teorem 3.3.1. *Ako vrijedi Zermelov teorem, tj. tvrdnja Teorema 3.1.2, tada vrijedi tvrdnja aksioma izbora (Aksioma 0.0.2).*

Dokaz. Neka je X skup nepraznih, u parovima disjunktnih skupova. Promatrajmo skup $\mathcal{X} := \bigcup_{Y \in X} Y$. Tada postoji dobar uređaj na $\mathcal{X}$. Označimo ga s R. Za $\emptyset \neq S \subseteq \mathcal{X}$ definiramo

$\min S$ kao R-najmanji element od S (koji postoji jer je R dobar uređaj). Definiramo skup $B := \{\min Y \mid Y \in X\}$. Neka je $Y \in X$ proizvoljan. Jasno je da je $\min Y \in B \cap Y$. Također zbog disjunktnosti elemenata od X slijedi da je $\min Y$ jedini element presjeka, tj. da je $B \cap Y = \{\min Y\}$. Uistinu, pretpostavimo da $B \cap Y$ nije jednočlan, tj. postoji neki $x \in B \cap Y$ takav da $x \neq \min Y$. Uočimo najprije da sada imamo $x \in Y$. Nadalje, po definiciji od B slijedi da postoji $Z \in X$ takav da je $x = \min Z$. Zbog $x \neq \min Y$ mora biti $Y \neq Z$. No, sada $\min Z \in Z$ i $\min Z \in Y$ znači da je $\min Z \in Y \cap Z$, što je nemoguće jer su Y i Z disjunktni. Dakle, $B \cap Y = \{\min Y\}$, kao što smo najavili. Drugim riječima, B je izborni skup za X. $\square$

Bibliografija

[1] B. Russell, *Introduction to mathematical philosophy*, Dover Publications, 1993 (engleski).

[2] Š. Ungar, *Uvod u teoriju skupova i matematičku logiku*, 2016. (pristupljeno 11. lipnja 2020.), `https://www.mathos.unios.hr/~sime/HR/skupovi/skupovi.pdf`.

[3] M. Vuković, *Teorija skupova, predavanja*, 2015.

Sažetak

Ukratko, u ovome radu se bavimo Zornovom lemom i srodnim tvrdnjama. U uvodu je obrazloženo zašto je naglasak na Zornovoj lemi.

U prvom poglavlju je precizno iskazan aksiom izbora, nabrojane su neke njemu ekvivalentne tvrdnje i neke njegove posljedice. Navedene su i neke posljedice aksioma izbora iz raznih grana matematike (linearne algebre, topologije, analize, i tako dalje).

U drugom poglavlju najprije definiramo pojmove potrebne za razumijevanje iskaza Zornove leme (parcijalno uređen skup, lanac, i slično). Nakon toga precizno iskazujemo Zornovu lemu, te je dokazujemo pod pretpostavkom aksioma izbora. Osim toga, iznosimo i nekoliko primjera upotrebe Zornove leme.

U trećem poglavlju se bavimo još jednim važnim teoremom teorije skupova: Zermelovim teoremom o dobrom uređaju. Preciznije, dokazujemo da Zornova lema povlači Zermelov teorem o dobrom uređaju. Na kraju poglavlja dokazujemo da Zermelov teorem povlači aksiom izbora.

Summary

In this paper, we present Zorn's lemma and some of its related statements. The introduction explains why the emphasis is on Zorn's lemma.

In the first chapter, we state the axiom of choice with some of its equivalent statements and consequences. We also state some consequences of axiom of choice from various branches of mathematics (linear algebra, topology, analysis, and so on).

In the second chapter we first define some terms which are needed to understand the statement of Zorn's lemma (partially ordered set, chain, and so on). Afterwards, we give a precise statement of Zorn's lemma and we prove it assuming the axiom of choice. We also provide a few examples of how Zorn's lemma can be used.

In the third chapter, we present another important theorem of set theory: the well-ordering theorem. We prove that Zorn's lemma implies the well-ordering theorem. At the end of this chapter, we prove that the well-ordering theorem implies the axiom of choice.

Životopis

Dana 25. studenog 1996. rođen sam u Karlovcu, gdje sam pohađao Osnovnu školu Dragojle Jarnević i Gimnaziju Karlovac. Već pri upisu u srednju školu sam se opredijelio za prirodoslovne predmete, pa sam pohađao prirodoslovno-matematičku gimnaziju.

2015. godine sam upisao Preddiplomski sveučilišni studij Matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu, koji sam 2018. godine i završio. Tada upisujem Diplomski sveučilišni studij Računarstva i matematike te Diplomski sveučilišni studij Financijske i poslovne matematike, oba na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu.