Cantorov skup i primjene

Brumnić, Tina

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Tina Brumnić

CANTOROV SKUP I PRIMJENE

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Maja Resman

Zagreb, rujan 2022.

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. _____

Ovaj rad posvećujem svojim roditeljima koji su mi bili iznimna podrška kroz čitav studij i nisu gubili vjeru u mene. Posebna zahvala mentorici izv. prof. dr. sc. Maji Resman na strpljenju i vremenu te velikoj stručnoj pomoći.

Sadržaj

Uvod

Tema ovoga rada je Cantorov ternarni skup. Cantorov ternarni skup dobiven je iterativnim uklanjanjem srednjih otvorenih trećina iz zatvorenog intervala na pravcu. Početnom zatvorenom intervalu $[0, 1]$ uklanja se srednja otvorena trećina $\langle 1/3, 2/3\rangle$ te preostaju dva zatvorena intervala $[0, 1/3]$ i $[2/3, 1]$. Cantorov skup je ono što preostaje u beskonačnom postupku uklanjanja srednjih otvorenih trećina. Veličina Cantorovog skupa je dvosmislena, odnosno, skup je istovremeno i „velik" i „mali". Naime, u Cantorovom skupu ima neprebrojivo mnogo točaka, ali ipak, on je duljine 0. U prvom je poglavlju detaljnije opisana geometrijska konstrukcija Cantorovog skupa te se određuje kardinalitet i duljina Cantorovog skupa.

Nadalje, u radu se pristupa Cantorovom skupu s aspekta teorije brojeva. U drugom se poglavlju daje jedna konstrukcija Cantorovog skupa pomoću verižnih razlomaka. Definiramo verižne razlomke i pokazujemo kako se realni brojevi zapisuju u obliku konačnih, odnosno beskonačnih, verižnih razlomaka. Kao primjenu, na kraju poglavlja dajemo konstrukciju Cantorovog skupa pomoću verižnih razlomaka.

U trećem se poglavlju Cantorov skup konstruira kao homeomorfna slika prstena p-adskih cijelih brojeva. Kreće se od definicije p-adske norme i p-adske udaljenosti na polju $\mathbb{Q}$, pokazuje se da ono nije potpuno u odnosu na definiranu normu, te se polje $\mathbb{Q}$ upotpunjuje do polja $\mathbb{Q}_p$. Elementi polja $\mathbb{Q}_p$, p-adski brojevi, definiraju se na dva ekvivalentna načina: kao klase ekvivalencije Cauchyjevih nizova, te pomoću p-adskih ekspanzija. Zapis u obliku jedinstvene p-adske ekspanzije omogućuje praktičnije izvođenje algebarskih operacija na skupu $\mathbb{Q}_p$, a iz p-adske se ekspanzije jednostavno prelazi na zapis pomoću Cauchyjevih klasa ekvivalencije, kao i obratno. Takva p-adska ekspanzija vodi do definicije skupa p-adskih cijelih brojeva $\mathbb{Z}_p$ kao potprostora $\mathbb{Q}_p$ koji ima strukturu prstena. Pokazujemo da je taj prostor homeomorfan Cantorovom skupu kao euklidskom potprostoru skupa $\mathbb{R}$.

Poglavlje 1

Uvod u Cantorov skup

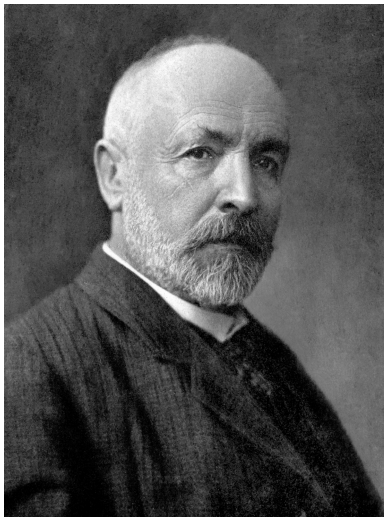
1.1 Povijesna bilješka o Georgu Cantoru

Ovo potpoglavlje napisano je prema [4], [14] i [17].
Iako nosi njegovo ime, Georg Cantor (1845.-1918.) nije bio prvi koji je definirao Cantorov skup. Henry J. S. Smith se 1875. godine bavio pitanjem integrabilnosti funkcija koje nisu neprekidne. Dok su primjeri integrabilnih funkcija koje imaju prekid u konačno mnogo točaka bili jednostavniji za konstruiranje, konstruirati primjer integrabilne funkcije s prekidima u beskonačno mnogo točaka bio je mnogo zahtjevniji pothvat. Smith je razvio metodu za konstrukciju takve funkcije. Dokazao je da je svaka funkcija koja se podudara s integrabilnom funkcijom svugdje osim na nigdje gustom skupu, integrabilna. Dao je nekoliko primjera nigdje gustog skupa, među kojima i Cantorov skup.
Godine 1881. Vito Volterra pokazao je kako konstruirati takav skup, no, njegov je rad zadobio malo pažnje. Konačno, 1883. godine, George Cantor daje konstrukciju koja će ovoga puta postati poznata. Cantorov primjer poznat je kao Cantorov ternarni skup.

Rođen 3. ožujka 1845. godine u St. Petersburgu u Rusiji, George Ferdinand Ludwig Philipp Cantor definirao je Cantorov skup isključivo aritmetičkim pristupom.
Nakon što se s obitelji, zbog očeve bolesti, odselio u Frankfurt, godine 1862. započinje srednjoškolsko obrazovanje na Federalnom Politehničkom Institutu u Zürichu. Nakon očeve smrti započinje studij na Sveučilištu u Berlinu, gdje su mu, između ostalih, profesori bili i Kronecker, Weierstrass te Kummer. Godine 1867. stječe doktorat znanosti s disertacijom „*De aequationibus secundi gradus interminatis*".

Uz temu ovoga rada, neke od njegovih najpoznatijih ideja su različiti tipovi beskonačnosti i hipoteza kontinuuma. George Cantor je uveo koncept *kardinalnosti* kako bi usporedio veličine beskonačnih skupova te je pokazao da je veličina skupa cijelih brojeva strogo manja od veličine skupa realnih brojeva.

Hipoteza kontinuuma tvrdi da ne postoji skup čija je veličina strogo između veličine skupa cijelih brojeva i veličine skupa realnih brojeva.



Slika 1.1: Georg Cantor (1845.-1918.)

1.2 Geometrijska konstrukcija Cantorovog skupa

Ovo potpoglavlje napisano je prema [17].
Postoji nekoliko načina na koje možemo konstruirati tzv. *Cantorov ternarni skup*. Opišimo jedan geometrijski način. Upravo se geometrijski, intuitivan pristup često koristi za predstavljanje elemenata Cantorovog skupa.

Krenemo od zatvorenog jediničnog intervala ($F_0 = [0, 1]$). Takav jedinični zatvoreni interval razdijelimo na tri jednaka dijela i uklonimo srednju otvorenu trećinu. Sada imamo $F_1 = [0, 1/3] \cup [2/3, 1]$. Dalje nastavljamo induktivno, pa se tako u n-tom koraku F_n sastoji od 2^n zatvorenih, disjunktnih podintervala duljine $\frac{1}{3^n}$. U koraku $n + 1$ ponovno svaki od 2^n intervala dijelimo na tri jednaka dijela od kojih uklanjamo srednju otvorenu trećinu. U limesu kad $n \to \infty$, ovaj postupak nas dovodi do padajuće familije skupova $\{F_n\}_{n=0}^{\infty}$, gdje je $F_n \supset F_{n+1}, n \in \mathbb{N}$. Cantorov skup definiran je kao *padajući presjek*:

$$C_{\frac{1}{3}} = \bigcap_{n=0}^{\infty} F_n.$$

Prva četiri koraka konstrukcije prikazana su na slici 1.2

Slika 1.2: Prva četiri koraka konstrukcije Cantorovog skupa

Postavlja se pitanje: koje točke (i koliko njih) ostaju u $C_{\frac{1}{3}}$? S obzirom na to da uklanjamo samo otvorene intervale bez rubnih točaka, očito je da u $C_{\frac{1}{3}}$ ostaju sve rubne točke intervala.

Primijetimo da smo ovom konstrukcijom, odnosno uklanjanjem otvorenih trećina intervala, definirali tzv. *ternarni* Cantorov skup. No, u konstrukciji nije nužno da uklanjamo trećine. Omjer uklonjenih otvorenih intervala i danih zatvorenih intervala označimo s r, gdje je $0 < r < 1$. Dani zatvoreni interval označimo s I, a intervale koje uklanjamo označimo s J. Omjer koji računamo dan je s

$$\frac{\ell(J)}{\ell(I)} = r,$$

gdje $\ell(\cdot)$ označava duljinu intervala. Tako dobiven Cantorov skup označavamo s C_r.

Također, moguća je sljedeća, još općenitija konstrukcija:
Dani zatvoreni interval podijelimo na tri dijela pri čemu zadržavamo dva vanjska dijela dok unutarnji otvoreni interval uklanjamo. Pri tome nije nužno da omjer duljina zadržanih dijelova bude 1. Posebno, svaki zatvoreni interval I podijeljen je na intervale I_0, M i I_1, gdje I i I_0 dijele lijevu rubnu točku, dok I i I_1 dijele desnu rubnu točku te vrijedi:

$$\frac{\ell(I_0)}{\ell(I)} = r_1$$

i

$$\frac{\ell(I_1)}{\ell(I)} = r_2,$$

uz $r_1 + r_2 < 1$.

U ovome radu naglasak je na Cantorovom ternarnom skupu, $C_{\frac{1}{3}}$, te će se u nastavku ispuštati riječ *ternarni* onda kada je jasno na koji se skup misli.

Promotrimo koje točke ostaju u Cantorovom skupu $C_{\frac{1}{3}}$. Promatramo decimalne brojeve između 0 i 1 zapisane u bazi 3. Lijevi se interval sastoji od brojeva čija je prva znamenka nakon ternarne točke jednaka 0, srednji interval sadrži brojeve koji nakon ternarne točke imaju znamenku 1, dok u desnom intervalu nalazimo sve brojeve koji nakon ternarne točke imaju znamenku 2.

Uklanjanje srednjeg intervala zapravo znači uklanjanje svih brojeva čija je prva znamenka nakon ternarne točke jednaka 1. U drugom koraku postupka, dijeljenjem lijevog i desnog intervala na tri dijela i potom uklanjanja sredine, uklanjaju se brojevi koji na drugom mjestu nakon ternarne točke imaju znamenku 1. Trećim korakom uklanjamo sve brojeve kojima je jedinica na trećem mjestu nakon ternarne točke. Nastavljanjem ovog postupka svi brojevi koji sadrže znamenku 1 bit će uklonjeni. Preostat će skup svih brojeva u skupu $[0, 1]$ koji nemaju znamenku 1 u svom ternarnom decimalnom prikazu.

Poseban oprez potreban je s rubnim točkama. Primjerice, u bazi 10 vrijedi

$$1.999999\ldots = 2.000000\ldots$$

Tako npr. $\frac{1}{3}$ u bazi 3 možemo zapisati na sljedeći način:

$$\frac{1}{3} = (0.1)_3,$$

no, $\frac{1}{3}$ je rubna točka pa se ipak mora nalaziti u Cantorovom skupu. Primijetimo da je $\frac{1}{3}$ moguće zapisati samo pomoću znamenaka 0 i 2.

$$\frac{1}{3} = (0.1)_3 = (0.1000\ldots)_3 = (0.0222\ldots)_3.$$

Vrijedi

$$(0.0222\ldots)_3 = 0 \cdot 3^{-1} + 2 \cdot 3^{-2} + 2 \cdot 3^{-3} + \ldots = 3^{-2}(2 + 2 \cdot 3^{-1} + 2 \cdot 3^{-2} + \ldots).$$

Koristeći formulu za sumu geometrijskog reda sada imamo:

$$3^{-2}(2 + 2 \cdot 3^{-1} + 2 \cdot 3^{-2} + \ldots) = \frac{1}{3^2} \cdot \frac{2}{1 - \frac{1}{3}} = \frac{1}{3^2} \cdot 3 = \frac{1}{3},$$

pa pišemo $(0.0222...)_3 = \left(\frac{1}{3}\right)_{10}$.

Slično,

$$(0.2222\ldots)_3 = 2\cdot 3^{-1} + 2\cdot 3^{-2} + 2\cdot 3^{-3} + \ldots = 3^{-1}(2 + 2\cdot 3^{-1} + 2\cdot 3^{-2} + \ldots)$$
$$= \frac{1}{3}\cdot 3 = 1_{10},$$

pa je $1_{10} = 1_3 = (0.2222\ldots)_3$.

1.2.1 Duljina Cantorovog skupa

Sljedeći teorem daje nam prvu dihotomiju vezanu uz Cantorov skup. Naime, u Cantorovom skupu ostaje beskonačno mnogo točaka, što ćemo pokazati u Potpoglavlju 1.3, čak neprebrojivo mnogo. Ipak, njegova duljina (Lebesgueova mjera) je 0. Tako je Cantorov skup istovremeno i „velik" i „mali".

Teorem 1.2.1 ([17])**.** *Duljina Cantorovog skupa $C_{\frac{1}{3}}$ jednaka je* 0*.*

Dokaz. Dokažimo da je ukupna duljina uklonjenih intervala iz $C_{\frac{1}{3}}$ jednaka 1. Iz toga slijedi tvrdnja teorema.
U svakom koraku $n > 0$ uklanjamo 2^{n-1} otvorenih intervala duljine $\left(\frac{1}{3}\right)^n$. Ukupnu duljinu svih uklonjenih otvorenih intervala možemo izračunati kao sumu geometrijskog reda

$$\sum_{n=1}^{\infty} 2^{n-1}\frac{1}{3^n}.$$

S obzirom na to da je $|q| < 1$, odnosno $\left|\frac{1}{3}\right| < 1$, znamo da taj red konvergira.
Vrijedi

$$\sum_{n=1}^{\infty} 2^{n-1}\frac{1}{3^n} = \frac{1}{3} + \frac{2}{3}\cdot\frac{1}{3} + \frac{2}{3}\cdot\frac{2}{9} + ... = \frac{\frac{1}{3}}{1-\frac{2}{3}} = 1.$$

□

Dakle, počevši od zatvorenog intervala duljine 1, u beskonačno mnogo koraka, uklonjeni su intervali ukupne duljine 1, no, u Cantorovom je skupu još uvijek preostalo beskonačno mnogo točaka. Unatoč tome, prema Teoremu 1.2.1, Cantorov skup je skup duljine nula.

1.3 Kardinalitet Cantorovog skupa

Važno pitanje u opisu Cantorovog skupa njegov je kardinalitet (je li konačan, prebrojiv, neprebrojiv...). Uz duljinu (Lebesgueovu mjeru), kardinalitet možemo smatrati *indikatorom* veličine Cantorovog skupa.

1.3.1 Kardinalitet skupa

Znamo za konačan skup A od k elemenata kažemo da je *kardinaliteta* k, i pišemo $\text{card}(A) = k$. Beskonačne skupove dijelimo na *prebrojivo beskonačne* i *neprebrojivo beskonačne*, a sukladno tome, razlikovat ćemo i njihove kardinalitete.

Cantorov rad otvorio je put ideji o *različitim tipovima beskonačnosti*. Prvo definirajmo pojam *ekvipotentnosti* skupova.

Definicija 1.3.1 ([17])**.** *Neka su A i B skupovi. Kažemo da su skupovi A i B ekvipotentni ako postoji bijekcija $f : A \to B$. Oznaka: $A \simeq B$.*

Tako vidimo da je $\text{card}(A) = k$ ako i samo ako $A \simeq \{1, 2, ..., k\}$.

Definicija 1.3.2 ([17])**.** *Za skup A kažemo da je prebrojiv ako je ili konačan ili ekvipotentan $\mathbb{N}$. Za skupove ekvipotentne $\mathbb{N}$ kažemo da su prebrojivo beskonačni. Ako skup nije prebrojiv, onda kažemo da je neprebrojiv.*

Kardinalitet beskonačnog skupa označavamo hebrejskim slovom *aleph* ($\aleph$). Kardinalitet prebrojivo beskonačnih skupova označava se s $\aleph_0$. Kardinalitet (neprebrojivog) skupa $\mathbb{R}$ označavamo s $2^{\aleph_0}$ ili $\mathfrak{c}$ i zovemo *kontinuum*.

Teorem 1.3.3 ([15])**.** *Jedinični interval* $[0, 1]$ *je neprebrojiv i kardinalitet mu je* $2^{\aleph_0}$.

Dokaz. Dokažimo da je $[0, 1] \simeq \mathbb{R}$. Dovoljno je pokazati da je $\langle -1, 1\rangle \simeq \mathbb{R}$, tj. da postoji bijekcija $f : \langle -1, 1\rangle \to \mathbb{R}$. Naime, očito postoji bijekcija $h : \langle 0, 1\rangle \to \langle -1, 1\rangle$ dana s $h(x) = 2x - 1$. Kompozicija $f \circ h$ je tada bijekcija s $\langle 0, 1\rangle$ na $\mathbb{R}$.
Definirajmo $f : \langle -1, 1\rangle \to \mathbb{R}$ s

$$f(x) = \frac{x}{1 - |x|}.$$

Tvrdimo da je f bijekcija. Pretpostavimo da su $x, y \in \langle -1, 1\rangle$ takvi da je $f(x) = f(y)$. Imamo

$$\frac{x}{1 - |x|} = \frac{y}{1 - |y|}, \tag{1.1}$$

pa je

$$x - x|y| = y - y|x|. \tag{1.2}$$

Iz $1 - |x| > 0, 1 - |y| > 0$ i (1.1), slijedi da su x i y istog predznaka. Ako su oba negativnog predznaka, vrijedi: $-x| - y| = -y| - x|$, a ako su oba pozitivnog predznaka, tada je $x|y| = y|x|$. Dakle, u oba slučaja je $x|y| = y|x|$, pa, iz (1.2), zaključujemo da je $x = y$. Time smo dokazali da je f injekcija.

Dokažimo sada surjektivnost.
Neka je $y \in \mathbb{R}$. Definirajmo

$$x = \frac{y}{1 + |y|}.$$

Očito je $|x| < 1$, tj. $x \in \langle -1, 1 \rangle$.

Sada vrijedi

$$f(x) = f\left(\frac{y}{1 + |y|}\right) = \frac{\frac{y}{1+|y|}}{1 - \frac{|y|}{1+|y|}} = \frac{\frac{y}{1+|y|}}{\frac{1}{1+|y|}} = y.$$

Dakle, postoji $x \in \langle -1, 1 \rangle$ takav da je $f(x) = y$, pa je f surjekcija.

Time smo dokazali da je $\text{card}(\langle 0, 1 \rangle) = \text{card}(\mathbb{R}) = 2^{\aleph_0}$. Kako $[0, 1]$ dobivamo od $\langle 0, 1 \rangle$ dodavanjem dviju točaka, te kako je $[0, 1] \subseteq \mathbb{R}$, a $\text{card}(\mathbb{R}) = 2^{\aleph_0}$, zaključujemo da je i $\text{card}([0, 1]) = 2^{\aleph_0}$, tj. da je $[0, 1]$ neprebrojiv. □

Teorem 1.3.4 ([17])**.** *Kardinalitet Cantorovog skupa je* $2^{\aleph_0}$.

Dokaz. Već smo vidjeli u Potpoglavlju 1.2 da se jedna reprezentacija Cantorovog skupa sastoji od ternarnih decimalnih brojeva iz intervala $[0, 1]$ koji se mogu zapisati samo pomoću znamenaka 0 i 2. Takve nizove možemo poistovjetiti s binarnim nizovima. Binarnu znamenku 1 zamijenimo znamenkom 2.

Konstruiramo funkciju $f : C_{\frac{1}{3}} \to [0, 1]$. Koristimo opisanu binarnu reprezentaciju brojeva u $[0, 1]$.

Neka je $x \in C_{\frac{1}{3}}$. Tada je $x = 0.a_1a_2a_3 \ldots, a_i \in \{0, 2\}$. Sad poistovjetimo ternarni zapis $0.a_1, \ldots, a_i$, kojeg zapišemo kao $0.a_1, \ldots, a_i, 0, 0, 0, 0, 0, \ldots$ s nizom nula i jedinica $b_1, b_2, \ldots, b_i, 0, 0, 0, \ldots$, gdje je

$$b_i = \begin{cases} 0, & za\ a_i = 0, \\ 1, & za\ a_i = 2. \end{cases}$$

Sada je dovoljno pokazati da svih nizova nula i jedinica ima neprebrojivo mnogo.
Pretpostavimo suprotno, tj. da ih ima prebrojivo mnogo. Tada postoji bijekcija između skupa $\mathbb{N}$ i tih nizova, pa ih možemo poredati u niz nizova. Formiramo novi niz nula i jedinica tako da mu je prvi element 0, ako je prvi element prvog niza bio 1 i obratno. Drugi element mu je 0 ako je drugi element drugog niza 1 ili obratno. Tako nastavimo dijagonalno i formiramo novi niz koji se očito razlikuje od svih nizova nula i jedinica te dobivamo kontradikciju. Dakle, takvih nizova nula i jedinica ima neprebrojivo mnogo. □

1.3.2 Gustoća Cantorovog skupa u [0, 1]

Prebrojivi skupovi su u nekom smislu mali, dok su neprebrojivi skupovi veliki. Još jedan indikator veličine skupa jest *gustoća* skupa. Gustoća skupa je topološki pojam, pa uvedimo prvo definiciju topologije.

Definicija 1.3.5 (Topologija, [17])**.** Topološkim prostorom *zovemo skup S zajedno s familijom τ podskupova skupa S ako je zadovoljeno:*

(i) $\emptyset, S \in \tau$,

(ii) *Ako je $U_\alpha \in \tau$ za svaki $\alpha \in A$, gdje je A skup indeksa, onda je $\bigcup_{\alpha\in A} U_\alpha \in \tau$,*

(iii) *Ako su $U, V \in \tau$, onda je $U \cap V \in \tau$.*

Elemente familije τ zovemo otvoreni skupovi *u S, a za τ kažemo da je* topologija *na S.* Topološkim prostorom *smatramo uređeni par (S, τ).*

Definicija 1.3.6 (Zatvoreni skup, [17])**.** *Kažemo da je skup V* zatvoren *u topološkom prostoru (S, τ) ako mu je komplement $V^c = S \setminus V$ otvoren, odnosno, $V^c \in \tau$.*

Definicija 1.3.7 (Gust skup, [17])**.** *Neka je (S, τ) topološki prostor i neka je $A \subseteq S$. Kažemo da je A* gust u *S ako za svaki $U \in \tau$ postoji $a \in A$ takav da $a \in U$. Odnosno, ako svaki otvoreni skup sadrži najmanje jednu točku iz A.*

Definicija 1.3.8 (Rijedak ili nigdje gust skup, [17])**.** *Neka je (S, τ) topološki prostor i neka je $B \subseteq S$. Kažemo da je B* nigdje gust u *S ako za svaki neprazan otvoreni skup $U \subseteq S$ postoji neprazan otvoreni skup V takav da*

$$V \subseteq U \quad \text{i} \quad V \cap B = \emptyset.$$

Primijetimo da je za sve ove definicije potrebno prvo definirati koju topologiju gledamo na prostoru. Mi ćemo na $\mathbb{R}$ promatrati euklidsku topologiju, a na svim podskupovima, uključujući Cantorov skup, relativnu topologiju induciranu euklidskom topologijom na $\mathbb{R}$. Sljedeći teorem pokazuje da je Cantorov skup, iako „velik" u smislu neprebrojivosti, topološki „mali" u euklidskoj topologiji.

Teorem 1.3.9 ([17])**.** *Cantorov skup je nigdje gust skup na realnom pravcu s euklidskom topologijom.*

Dokaz. Neka je I proizvoljan otvoreni interval na realnom pravcu (bazni skup euklidske topologije). Dovoljno je tvrdnju iz Definicije 1.3.8 pokazati za bazne intervale, jer svaki otvoreni skup $U \subseteq \mathbb{R}$ sadrži neki bazni interval. Tada postoji $k \in \mathbb{Z}$ takav da je $3^{-k} < \ell(I)$, gdje je $\ell(I)$ duljina intervala I. Prisjetimo se da u k-tom koraku konstrukcije Cantorovog skupa u skupu F_k ostaju disjunktni zatvoreni intervali duljine najviše 3^{-k}, te da je komplement, F_k^c, otvoren, jer smo uklonili konačno mnogo otvorenih intervala. Stoga je, zbog $\ell(I) > 3^{-k}$, $I \cap F_k^c$ neprazan (i otvoren zbog otvorenosti oba skupa u presjeku), pa postoji interval $J \subseteq I$ takav da je $J \subseteq F_k^c$, a tada je J pogotovo podskup komplementa Cantorovog skupa koji je jednak $\cup_{k\in\mathbb{N}} F_k^c$. Dakle, $J \subseteq I$ nema presjeka s Cantorovim skupom. □

Poglavlje 2

Cantorov skup i verižni razlomci

2.1 Uvod u verižne razlomke

Definicija 2.1.1 (Verižni razlomci, [10])**.** *Neka su a_i, b_i, $i \in \mathbb{N}_0$, realni brojevi, uz $a_i > 0$, za $i \geq 1$. Izraz oblika*

$$a_0 + \cfrac{b_0}{a_1 + \cfrac{b_1}{a_2 + \cfrac{b_2}{a_3 + \ddots}}}$$

nazivamo (beskonačni) verižni razlomak. *Brojevi a_i nazivaju se* parcijalni kvocijenti verižnog razlomka. *Verižni razlomak s konačno mnogo parcijalnih kvocijenata naziva se* konačni verižni razlomak.

Definicija 2.1.2 (Jednostavni verižni razlomci, [10])**.** *Neka je a_0 cijeli broj, a a_i, za $i \in \mathbb{N}$, prirodni brojevi. Izraz oblika*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \tag{2.1}$$

nazivamo jednostavni verižni razlomak.

Izraz (2.1) kraće zapisujemo kao $[a_0 : a_1, a_2, a_3, \ldots]$. Vrijednosti $a_0, a_1, a_2, \ldots$ su parcijalni kvocijenti verižnog razlomka.

Primjer 2.1.3. *Zapišimo jednostavni konačni verižni razlomak* $[1 : 2, 3, 2]$ *kao racionalan broj.*

Rješenje:

$$1+\frac{1}{2+\frac{1}{3+\frac{1}{2}}}=1+\frac{1}{2+\frac{1}{\frac{7}{2}}}=1+\frac{1}{2+\frac{2}{7}}=1+\frac{1}{\frac{16}{7}}=1+\frac{7}{16}=\frac{23}{16}.$$

Sređivanjem konačnog verižnog razlomka dobiva se racionalan broj. Dakako, vrijedi i obrat (Teorem 2.1.4). Svaki racionalni broj $x=\frac{p}{q}$, $p, q \in \mathbb{Z}$, $q \neq 0$, može se zapisati kao konačan verižni razlomak. Takav postupak zovemo *razvoj broja* $x \in \mathbb{Q}$ *u verižni razlomak.*

Teorem 2.1.4 ([5])**.** *Svaki konačni jednostavni verižni razlomak moguće je prikazati kao racionalni broj. Obratno, svaki racionalni broj moguće je prikazati kao konačni jednostavni verižni razlomak.*

Dokaz. Prvu tvrdnju dokazujemo matematičkom indukcijom. Primijetimo da vrijedi $[a_0 :] = a_0$, $a_0 \in \mathbb{Z} \subseteq \mathbb{Q}$. Pokažimo da vrijedi baza indukcije za $n = 1$.

$$[a_0 : a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$$

Iz definicije 2.1.2 vrijedi da je a_0 cijeli, a a_1 prirodni broj, pa zaključujemo da je $\frac{a_0 a_1+1}{a_1}$ racionalni broj.
Pretpostavimo da je $[a_1 : a_2, a_3, \ldots, a_n]$ racionalni broj, za $a_i \in \mathbb{N}$.
Tada vrijedi:

$$[a_0 : a_1, a_2, \ldots, a_n] = a_0 + \frac{1}{[a_1 : a_2, a_3, \ldots, a_n]}.$$

Prema pretpostavci, $[a_1 : a_2, a_3, \ldots, a_n]$ je racionalni broj. Dakle, $[a_1 : a_2, a_3, \ldots, a_n] = \frac{p}{q}$, za neke $p \in \mathbb{Z}$, $q \in \mathbb{N}$. Sada je

$$a_0 + \frac{1}{[a_1 : a_2, a_3, \ldots, a_n]} = a_0 + \frac{q}{p} = \frac{a_0 p + q}{p},$$

što je očito racionalni broj te vrijedi korak indukcije. Time je tvrdnja dokazana. Preostaje pokazati obrat tvrdnje.
Neka je $\frac{p}{q}$ racionalni broj, uz $q > 0$. Matematičkom indukcijom pokažimo da se $\frac{p}{q}$ može zapisati kao konačan verižni razlomak. Tvrdnju ponovno dokazujemo indukcijom po $q \in \mathbb{N}$. Za $q = 1$ vrijedi

$$\frac{p}{q} = p = [p :].$$

Pretpostavimo da je racionalni broj s nazivnikom manjim od q, $q > 1$, moguće zapisati kao konačni jednostavni verižni razlomak. Pokažimo da tada i racionalni broj s nazivnikom q možemo zapisati kao konačan jednostavni verižni razlomak. Koristeći teorem o dijeljenju s ostatkom, p možemo zapisati kao

$$p = qa_0 + r, \tag{2.2}$$

gdje su a_0, $r \in \mathbb{Z}$ i vrijedi $0 \leq r < q$. Dijeljenjem jednakosti (2.2) s q slijedi

$$\frac{p}{q} = a_0 + \frac{r}{q}.$$

Sada razlikujemo dva slučaja:

1° $r = 0$. Tada je $\frac{p}{q} = a_0 = [a_0 :]$, a $a_0 \in \mathbb{Z}$, pa tvrdnja vrijedi.
2° $r \neq 0$. Vrijedi

$$\frac{p}{q} = a_0 + \frac{1}{\frac{q}{r}}. \tag{2.3}$$

gdje je $q \in \mathbb{N}$ i $r < q$.
Kako je $r < q$, te q, $r \in \mathbb{N}$, koristeći pretpostavku indukcije vrijedi:

$$\frac{q}{r} = [b_1 : b_2, b_3, \ldots, b_n],$$

za neke $b_1, ..., b_n \in \mathbb{N}$.
Iz (2.3) slijedi

$$\frac{p}{q} = a_0 + \frac{1}{[b_1 : b_2, b_3, \ldots, b_n]} = [a_0 : b_1, b_2, \ldots, b_n].$$

Time je dokazan obrat tvrdnje.

□

Također, dokaz obrata nam daje i „algoritam" za zapis racionalnog broja u obliku verižnog razlomka korištenjem teorema o dijeljenju s ostatkom.

Primjer 2.1.5. *Razvijmo broj $\frac{118}{83}$ u konačni jednostavni verižni razlomak.*

Rješenje:

$$\begin{aligned} 118 &= 83 \cdot 1 + 35 \\ 83 &= 35 \cdot 2 + 13 \\ 35 &= 13 \cdot 2 + 9 \\ 13 &= 9 \cdot 1 + 4 \\ 9 &= 4 \cdot 2 + 1 \\ 4 &= 1 \cdot 4 \end{aligned}$$

Odavde je

$$\frac{118}{83} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{4}}}}} = [1 : 2, 2, 1, 2, 4].$$

Primjer 2.1.6. *Razvijmo broj* $-\frac{118}{83}$ *u konačni jednostavni verižni razlomak.*

Rješenje:

$$\begin{aligned} -118 &= 83 \cdot (-2) + 48 \\ 83 &= 48 \cdot 1 + 35 \\ 48 &= 35 \cdot 1 + 13 \\ 35 &= 13 \cdot 2 + 9 \\ 13 &= 9 \cdot 1 + 4 \\ 9 &= 4 \cdot 2 + 1 \\ 4 &= 1 \cdot 4 \end{aligned}$$

Odavde je

$$-\frac{118}{83} = -2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{4}}}}}} = [-2 : 1, 1, 2, 1, 2, 4].$$

Primijetimo da zapis racionalnog broja u obliku jednostavnog verižnog razlomka nije jedinstven. Neka racionalni broj $\frac{p}{q}$, $p, q \in \mathbb{Z}$, $q > 0$, ima prikaz $[a_0 : a_1, a_2, \ldots, a_n]$ kao

verižni razlomak. Posljednji parcijalni kvocijent u prikazu a_n, $a_n > 1$, moguće je zapisati kao

$$\frac{1}{a_n} = \frac{1}{(a_n - 1) + \frac{1}{1}},$$

pa $\frac{p}{q}$ možemo zapisati i kao

$$\frac{p}{q} = [a_0, a_1, \ldots, a_n - 1, 1].$$

Lema 2.1.7 ([7]). *Neka je $\frac{p}{q}$, $p \in \mathbb{Z}$, $p \neq 0$, $q \in \mathbb{N}$, racionalni broj. Tada $\frac{p}{q}$ ima točno dva razvoja u jednostavni verižni razlomak. Jedan je oblika $[a_0 : a_1, a_2, \ldots, a_n]$ uz $a_n \geq 2$, a drugi je oblika $[a_0 : a_1, a_2, \ldots, a_{n-1}, a_n - 1, 1]$.*

Dokaz. Skratimo razlomak $\frac{p}{q}$ do kraja, tako da su p, q relativno prosti brojevi. Prema Teoremu 2.1.4, $\frac{p}{q}$ ima razvoj u jednostavni verižni razlomak $\frac{p}{q} = [a_0 : a_1, a_2, \ldots, a_n]$, gdje je $a_0 \in \mathbb{Z}$, a $a_1, a_2, \ldots, a_n \in \mathbb{N}$. Lemu dokazujemo matematičkom indukcijom po q.

Ako je $q = 1$, tvrdnju dokazujemo za cijeli broj $p \neq 0$. Razlikujemo dva slučaja:

1° Za $n = 0$, imamo $p = [a_0] = a_0$, pa je $p = [p]$.
2° Za $n > 0$, prema Teoremu 2.1.4 je,

$$p = a_0 + \frac{1}{[a_1 : a_2, \ldots, a_n]}$$

i $[a_1 : a_2, \ldots, a_n] \geq 1$. Naime, ako razvijemo broj $\frac{p}{q}$ u verižni razlomak, tada je član a_0 jednoznačno određen kao cijeli dio broja $\frac{p}{q}$. Kako je $p - a_0 \in \mathbb{Z}$, slijedi $[a_1 : a_2, \ldots, a_n] = 1$. S obzirom da je $a_1 \geq 1$, zaključujemo da je $n = 1$ i $a_1 = 1$. Stoga je jedan zapis $p = [a_0 : 1]$. Tada slijedi $a_0 = p - 1$, odnosno, $p = [p - 1, 1]$, pa baza indukcije vrijedi.

Pretpostavimo sada da tvrdnja vrijedi za sve prirodne brojeve manje od q, $q > 1$.
Primijetimo da za $q > 1$ mora biti $n > 0$ zbog pretpostavke da su p i q relativno prosti brojevi.
Zbog jednoznačnosti a_0 u razvoju $\frac{p}{q}$ kao najvećeg cijelog dijela broja $\frac{p}{q}$ imamo

$$\frac{p}{q} = a_0 + \frac{p_1}{q} = a_0 + \frac{1}{\frac{q}{p_1}},$$

gdje je $p_1 < q$, prema teoremu o dijeljenju cijelih brojeva s ostatkom. Prema pretpostavci indukcije, $\frac{q}{p_1}$ ima točno dva razvoja u jednostavni verižni razlomak. Jedan je oblika $[a_1 : a_2, \ldots, a_n]$ uz $a_n \geq 2$, a drugi oblika $[a_1 : a_2, \ldots, a_{n-1}, a_n - 1, 1]$. Time je tvrdnja dokazana. □

Primjer 2.1.8. *Odredimo dva razvoja racionalnog broja* $\frac{89}{37}$ *u jednostavni verižni razlomak.*

$$\frac{89}{37} = 2 + \frac{15}{37} = 2 + \frac{1}{\frac{37}{15}} = 2 + \frac{1}{2 + \frac{7}{15}} = 2 + \frac{1}{2 + \frac{1}{\frac{15}{7}}} = 2 + \frac{1}{2 + \frac{1}{2+\frac{1}{7}}} = [2 : 2, 2, 7].$$

$$\frac{89}{37} = 2 + \frac{15}{37} = 2 + \frac{1}{\frac{37}{15}} = 2 + \frac{1}{2 + \frac{7}{15}} = 2 + \frac{1}{2 + \frac{1}{\frac{15}{7}}} = 2 + \frac{1}{2 + \frac{1}{2+\frac{1}{7}}} = 2 + \frac{1}{2 + \frac{1}{2+\frac{1}{6+\frac{1}{1}}}} =$$
$$= [2 : 2, 2, 6, 1].$$

Primjer 2.1.9. *Odredimo racionalni broj čiji je razvoj u verižni razlomak* $[-2 : 1, 3, 2, 2, 3]$.

$$[-2 : 1, 3, 2, 2, 3] = -2 + \frac{1}{1 + \frac{1}{3+\frac{1}{2+\frac{1}{2+\frac{1}{3}}}}} = -2 + \frac{1}{1 + \frac{1}{3+\frac{1}{2+\frac{1}{\frac{7}{3}}}}} = -2 + \frac{1}{1 + \frac{1}{3+\frac{1}{2+\frac{3}{7}}}} =$$
$$= -2 + \frac{1}{1 + \frac{1}{3+\frac{1}{\frac{17}{7}}}} = -2 + \frac{1}{1 + \frac{1}{3+\frac{7}{17}}} = -2 + \frac{1}{1 + \frac{1}{\frac{58}{17}}} =$$
$$= -2 + \frac{1}{1 + \frac{17}{58}} = -2 + \frac{1}{\frac{75}{58}} = -2 + \frac{58}{75} = -\frac{92}{75}.$$

Definicija 2.1.10 ([17])**.** *Neka je* $[a_0 : a_1, a_2, a_3, \ldots]$, $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$, *za* $i \geq 1$, *jednostavni verižni razlomak (konačan ili beskonačan). Za svaki* $k \in \mathbb{N}_0$, *konačni jednostavni verižni razlomak* $[a_0 : a_1, a_2, \ldots, a_k]$ *nazivamo k-ta* konvergenta jednostavnog verižnog razlomka *i označavamo s* c_k.

$$c_0 = a_0, \quad c_1 = a_0 + \frac{1}{a_1}, \quad c_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}, \ldots$$

Općenito, $c_n = [a_0 : a_1, a_2, \ldots, a_n]$.

Uobičajeno, konvergente prikazujemo kao racionalne brojeve, $c_0 = a_0 = \frac{p_0}{q_0}$, $c_1 = a_0 + \frac{1}{a_1} = \frac{p_1}{q_1}$, $c_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{p_2}{q_2}$, itd., gdje su $p_i, q_i \in \mathbb{Z}, q_i \neq 0$.

Sljedeći teorem daje vezu između nizova $(p_n)_n$, $(q_n)_n$ i $(a_n)_n$.

Teorem 2.1.11 ([17]). *Neka je* $[a_0 : a_1, a_2, a_3, \ldots]$, $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$, *za* $i \geq 1$, *jednostavni verižni razlomak i neka su* $(p_i)_{i\in\mathbb{N}}$ *i* $(q_i)_{i\in\mathbb{N}}$ *nizovi definirani rekurzivno s*

$$p_i = a_i p_{i-1} + p_{i-2}, \tag{2.4}$$
$$q_i = a_i q_{i-1} + q_{i-2}, \tag{2.5}$$

$i \in \mathbb{N}, i \geq 2$, *s početnim vrijednostima*

$$p_0 = a_0, \qquad p_1 = a_1 a_0 + 1,$$
$$q_0 = 1, \qquad q_1 = a_1.$$

Tada je i-ta konvergenta jednostavnog verižnog razlomka, c_i, $i \in \mathbb{N}_0$, *dana s* $c_i = \frac{p_i}{q_i}$.

Dokaz. Teorem dokazujemo induktivno po duljini konačnog verižnog razlomka.
Baza indukcije se provjerava za sve verižne razlomke $[a_0 :]$ i $[a_0 : a_1]$.
Za $i = 0$ vrijedi $c_0 = a_0 = \frac{a_0}{1} = \frac{p_0}{q_0}$, a za $i = 1$ vrijedi $c_1 = a_0 + \frac{1}{a_1} = \frac{(a_1 a_0 + 1)}{a_1} = \frac{p_1}{q_1}$.
Za $i = 2$ imamo

$$c_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1} = \frac{a_2 p_1 + p_0}{a_1 q_1 + q_0} = \frac{p_2}{q_2},$$

pa tvrdnja vrijedi za $i = 2$.
Pretpostavimo da tvrdnja $c_i = \frac{p_i}{q_i}$ vrijedi za sve konačne verižne razlomke duljine $i \leq k$ i dokažimo da je tada

$$c_{k+1} = \frac{p_{k+1}}{q_{k+1}}.$$

Vrijedi

$$c_{k+1} = [a_0 : a_1, a_2, \ldots, a_{k-1}, a_k, a_{k+1}] = \left[a_0 : a_1, a_2, \ldots, a_{k-1}, \left(a_k + \frac{1}{a_{k+1}}\right)\right].$$

Primijetimo da smo dobili verižni razlomak duljine k, pa, koristeći pretpostavku indukcije, vrijedi:

$$\left[a_0 : a_1, a_2, \ldots, \left(a_k + \frac{1}{a_{k+1}}\right)\right] = \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} = \frac{(a_k a_{k+1} + 1) p_{k-1} + a_{k+1} p_{k-2}}{(a_k a_{k+1} + 1) q_{k-1} + a_{k+1} q_{k-2}} =$$
$$= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k-1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}.$$

Zaključujemo da korak indukcije vrijedi, te je time dokazana početna tvrdnja.

□

Napomena 2.1.12. *Dogovorno uzimamo da je* $p_{-2} = 0$ *i* $p_{-1} = 1$*, te* $q_{-2} = 1$ *i* $q_{-1} = 0$*, s time da* $\frac{p_{-2}}{q_{-2}}$ *i* $\frac{p_{-1}}{q_{-1}}$ *nisu konvergente.*

Lema 2.1.13 ([7])**.** *Za* $i \in \mathbb{Z}$*,* $i \geq -1$ *vrijedi*

$$q_i p_{i-1} - p_i q_{i-1} = (-1)^i,$$

gdje su nizovi $(p_i)_i$ *i* $(q_i)_i$ *definirani kao u Teoremu 2.1.11.*

Dokaz. Lemu dokazujemo matematičkom indukcijom po i.
Prema Napomeni 2.1.12, za $i = -1$ imamo $q_{-1}p_{-2} - p_{-1}q_{-2} = 0 \cdot 0 - 1 \cdot 1 = (-1)^{-1}$.
Pretpostavimo da tvrdnja vrijedi za $i - 1$ i dokažimo da tada vrijedi i za $i \in \mathbb{N}_0$. Prema Teoremu 2.1.11, vrijedi

$$\begin{aligned} q_i p_{i-1} - p_i q_{i-1} &= (a_i q_{i-1} + q_{i-2})p_{i-1} - (a_i p_{i-1} + p_{i-2})q_{i-1} \\ &= -(q_{i-1}p_{i-2} - p_{i-1}q_{i-2}) = -(-1)^{i-1} = (-1)^i. \end{aligned}$$

Dakle, korak indukcije vrijedi, pa je time tvrdnja dokazana.

□

Lema 2.1.14 ([7])**.** *Za* $i \in \mathbb{Z}$*,* $i \geq 0$*, vrijedi*

$$q_i p_{i-2} - p_i q_{i-2} = (-1)^{i-1} a_i,$$

gdje su nizovi $(p_i)_i$ *i* $(q_i)_i$ *definirani kao u Teoremu 2.1.11.*

Dokaz. Iz Teorema 2.1.11 i Leme 2.1.13 slijedi

$$\begin{aligned} q_i p_{i-2} - p_i q_{i-2} &= (a_i q_{i-1} + q_{i-2})p_{i-2} - (a_i p_{i-1} + p_{i-2})q_{i-2} \\ &= a_i(q_{i-1}p_{i-2} - p_{i-1}q_{i-2}) = (-1)^{i-1} a_i. \end{aligned}$$

□

Dodatno, koristeći Lemu 2.1.14 lako se dobije da, za $n \geq 0$, uz zapisivanje konvergenti pomoću nizova $\frac{(p_n)_n}{(q_n)_n}$ definiranih u (2.4) i (2.5), vrijedi:

$$\begin{aligned} c_n - c_{n-2} &= \frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{p_n q_{n-2} - p_{n-2} q_n}{q_n q_{n-2}} \\ &= \frac{-(p_{n-2}q_n - p_n q_{n-2})}{q_n q_{n-2}} = \frac{-(-1)^{n-1} a_n}{q_n q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}. \end{aligned} \tag{2.6}$$

Jednak rezultat, uz nešto više računa, dobili bismo i koristeći Lemu 2.1.13. Taj će nam rezultat koristiti u nastavku.

Teorem 2.1.15 ([7]). *Neka su $c_0, c_1, c_2, \ldots$ konvergente beskonačnog verižnog razlomka. Tada vrijedi:*

(i) $c_0 < c_2 < c_4 < \ldots$,

(ii) $c_1 > c_3 > c_5 > \ldots$,

(iii) *Ako je i paran, j neparan, onda je $c_i < c_j$, za svaki $i, j \in \mathbb{N}$.*

Dokaz. Kako su u definiciji verižnog razlomka parcijalni kvocijenti $a_i > 0$, za $i \in \mathbb{N}$, te za svaki član niza $(q_i)_{i\in\mathbb{N}_0}$ definiranog u (2.5) vrijedi $q_i > 0$, iz rezultata (2.6) slijedi da za $i \in \mathbb{N}$, $i \geq 2$ paran, vrijedi

$$c_i - c_{i-2} = \frac{a_i}{q_i q_{i-2}} > 0,$$

pa je $c_{i-2} < c_i$. S druge strane, za $j \in \mathbb{N}$, $j \geq 2$ neparan, vrijedi

$$c_j - c_{j-2} = -\frac{a_j}{q_j q_{j-2}} < 0,$$

pa je $c_{j-2} > c_j$. Time su tvrdnje (i) i (ii) dokazane, te preostaje dokazati tvrdnju (iii).

Neka je $i < j$. Kako je, prema pretpostavci, j neparan, $j - 1$ je paran i vrijedi $i \leq j - 1$. Tada je, prema tvrdnji (i), $c_i \leq c_{j-1}$. Dovoljno je dokazati da, za $j \in \mathbb{N}$ neparan, vrijedi $c_{j-1} < c_j$. Za p_i i q_i definirane kao u Teoremu 2.1.11 iz Leme 2.1.13 slijedi

$$\frac{p_j}{q_j} - \frac{p_{j-1}}{q_{j-1}} = \frac{(-1)^{j+1}}{q_{j-1}q_j},$$

iz čega zaključujemo da je

$$\frac{p_{j-1}}{q_{j-1}} < \frac{p_j}{q_j},$$

odnosno

$$c_{j-1} < c_j,$$

za j neparan. Time je dokazana tvrdnja (iii).

□

Sljedeći teorem kaže da niz konvergenti beskonačnog jednostavnog verižnog razlomka konvergira u $\mathbb{R}$.

Teorem 2.1.16 ([7]). *Neka je a_0 cijeli broj i $(a_i)_{i\geq 1}$ niz prirodnih brojeva. Tada je niz $(c_n)_n$,*

$$c_n := [a_0 : a_1, a_2, \ldots, a_n],$$

$n \in \mathbb{N}$, konvergentan u $\mathbb{R}$.

Dokaz. Budući da je prema Teoremu 2.1.15 $c_0 < c_2 < \ldots < c_1$, niz $(c_n)_n$ za n paran je rastući i odozgo omeđen s c_1, pa postoji

$$L_1 := \lim_{\substack{n\to\infty \\ n\ paran}} \frac{p_n}{q_n}.$$

Slično, kako je $c_1 > c_3 > \ldots > c_0$, postoji i

$$L_2 := \lim_{\substack{n\to\infty \\ n\ neparan}} \frac{p_n}{q_n},$$

gdje su nizovi $(p_n)_n$ i $(q_n)_n$ definirani relacijama (2.4) i (2.5). Prema Lemi 2.1.13, vrijedi

$$\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_{n-1}q_n}.$$

Kako je $(q_n)_{n\in\mathbb{N}}$ definiran relacijom (2.5) s početnim uvjetima definiranim u Teoremu 2.1.11 strogo rastući niz prirodnih brojeva ($a_i > 0$, za $i \in \mathbb{N}$), slijedi da je

$$\lim_{n\to\infty} \frac{(-1)^n}{q_{n-1}q_n} = 0.$$

Zaključujemo da su limesi L_1 i L_2 jednaki čime je dokazana tvrdnja teorema. □

Napomena 2.1.17. *Limes $x = \lim_{n\to\infty} c_n$ zovemo realnim brojem pridruženim verižnom razlomku i pišemo $x = [a_0 : a_1, a_2, \ldots]$. U Teoremu 2.1.20 pokazujemo i drugi smjer.*

U dokazu Teorema 2.1.20 koristimo sljedeću lemu.

Lema 2.1.18 ([7]). *Neka je $[a_0 : a_1, a_2, \ldots]$ jednostavni verižni razlomak i neka je $r_i = [a_i, a_{i+1}, a_{i+2}, \ldots]$, za $i \in \mathbb{N}$. Tada je*

$$[a_0 : a_1, a_2, \ldots] = [a_0 : a_1, a_2, \ldots, a_{i-1}, [a_i, a_{i+1}, \ldots]] = \frac{p_{i-1}r_i + p_{i-2}}{q_{i-1}r_i + q_{i-2}},$$

gdje su $(p_i)_i$, $(q_i)_i$ nizovi definirani kao u Teoremu 2.1.11.

Dokaz. Druga jednakost slijedi izravno iz Teorema 2.1.11. Prvu ćemo jednakost dokazati indukcijom po i. Provjerimo da tvrdnja vrijedi za $i = 1$:

$$[a_0 : a_1, a_2, \ldots] = a_0 + \frac{1}{[a_1 : a_2, a_3, \ldots]} = [a_0 : [a_1 : a_2, a_3, \ldots]].$$

Pretpostavimo sada da tvrdnja vrijedi za $i - 1$, gdje je $i > 1$. Tada je

$$[a_0 : a_1, a_2, \ldots] = a_0 + \frac{1}{[a_1 : a_2, a_3, \ldots]},$$

a prema pretpostavci indukcije je

$$\begin{aligned} a_0 + \frac{1}{[a_1 : a_2, a_3, \ldots]} &= a_0 + \frac{1}{[a_1 : a_2, \ldots, a_{i-2}, [a_{i-1} : a_i, a_{i+1}, \ldots]]} \\ &= a_0 + \frac{1}{\left[a_1 : a_2, \ldots, a_{i-2}, \left(a_{i-1} + \frac{1}{[a_i : a_{i+1}, a_{i+2}, \ldots]}\right)\right]} \\ &= a_0 + \frac{1}{[a_1 : a_2, \ldots, a_{i-1}, [a_i : a_{i+1}, a_{i+2}, \ldots]]} \\ &= [a_0 : a_1, \ldots, a_{i-1}, [a_i : a_{i+1}, a_{i+2}, \ldots]], \end{aligned}$$

pa tvrdnja vrijedi i za i. Time je pokazano da i prva jednakost vrijedi.

□

Napomena 2.1.19. *Primijetimo da za jednostavni verižni razlomak* $[a_0 : a_1, \ldots, a_n]$ *zapis* $[a_0 : a_1, \ldots, a_{i-1}, [a_i : a_{i+1}, \ldots]]$ *ne mora biti jednostavni verižni razlomak.*

Teorem 2.1.20 ([12])**.** *Svaki realan broj x moguće je razviti u jednostavni verižni razlomak, u smislu da konvergente verižnog razlomka konvergiraju k tom realnom broju.*

Dokaz. Označimo s a_0 najveći cijeli broj manji ili jednak x, tj.

$$a_0 = \lfloor x \rfloor.$$

Ako x nije cijeli broj, onda postoji $r_1 \in \mathbb{R}$, $r_1 > 1$, t.d.

$$x = a_0 + \frac{1}{r_1}. \tag{2.7}$$

Za $x - a_0$ očito vrijedi

$$0 < \frac{1}{r_1} = x - a_0 < 1.$$

Relaciju (2.7) možemo zapisati kao

$$x = [a_0 : r_1],$$

Sada definiramo prirodan broj

$$a_1 = \lfloor r_1 \rfloor.$$

Ponovno, ako r_1 nije cijeli broj, onda postoji $r_2 \in \mathbb{R}$, $r_2 > 1$, t.d.

$$r_1 = a_1 + \frac{1}{r_2} \tag{2.8}$$

Iz (2.7) i (2.8) slijedi

$$x = a_0 + \frac{1}{r_1} = a_0 + \frac{1}{a_1 + \frac{1}{r_2}},$$

tj.

$$x = [a_0 : a_1, r_2].$$

Ovaj postupak možemo ponavljati sve dok r_i, $i \geq 2$, nije prirodan broj. Dakle, ako $r_2, \ldots, r_{n-1}$ nisu prirodni brojevi, onda postoji $r_n > 1$, $r_n \in \mathbb{R}$, takav da je

$$x = [a_0 : a_1, a_2, \ldots, a_{n-1}, r_n].$$

U $(n+1)$-om koraku stavimo

$$a_n = \lfloor r_n \rfloor.$$

Ako je r_n prirodan broj, onda je $r_n - a_n = 0$ i postupak staje. Tada dobivamo da je

$$x = [a_0 : a_1, a_2, \ldots, a_{n-1}, a_n],$$

pa zaključujemo da je x racionalan broj.
Ako r_n nije prirodan broj, postupak se nastavlja. Tada je $0 < r_n - a_n < 1$ i za $r_{n+1} \in \mathbb{Z}$, $r_{n+1} > 1$, vrijedi

$$r_n = a_n + \frac{1}{r_{n+1}},$$

iz čega slijedi da je

$$x = [a_0 : a_1, a_2, \ldots, a_n, r_{n+1}],$$

i tako dalje.
Ukoliko postupak nikad ne staje, tj. r_i, $i \geq 2$, nikad ne postane prirodan broj, imat ćemo $x = [a_0 : a_1, a_2, \ldots]$, odnosno, dobit ćemo beskonačni verižni razlomak čije konvergente konvergiraju upravo realnom broju x. Dokažimo to.
Označimo s x_n n-tu konvergentu beskonačnog verižnog razlomka pridruženog realnom broju x, $n \in \mathbb{N}$. Dakle, $x_n = [a_0 : a_1, \ldots, a_n]$ je konačni verižni razlomak.
Neka su $(p_n)_n$ i $(q_n)_n$ nizovi definirani kao u Teoremu 2.1.11. Tada, n-tu konvergentu x_n možemo zapisati kao

$$x_n = \frac{p_n}{q_n},$$

Prema Lemi 2.1.18 imamo

$$x = \frac{p_{n-1}r_n + p_{n-2}}{q_{n-1}r_n + q_{n-2}}, \tag{2.9}$$

gdje r_n zadovoljava $x = [a_0 : a_1, \ldots, a_{n-1}, r_n]$, za $n \in \mathbb{N}$. S druge strane, prema Teoremu 2.1.11 možemo pisati

$$x_n = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}, \tag{2.10}$$

$n \in \mathbb{N}$. Sada, iz (2.9) i (2.10) slijedi

$$\begin{aligned} x - x_n &= \frac{p_{n-1}r_n + p_{n-2}}{q_{n-1}r_n + q_{n-2}} - \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} \\ &= \frac{(p_{n-1}r_n + p_{n-2})(a_n q_{n-1} + q_{n-2}) - (a_n p_{n-1} + p_{n-2})(q_{n-1}r_n + q_{n-2})}{(q_{n-1}r_n + q_{n-2})(a_n q_{n-1} + q_{n-2})} \\ &= \frac{(r_n - a_n)(p_{n-1}q_{n-2}) + (a_n - r_n)(p_{n-2}q_{n-1})}{(q_{n-1}r_n + q_{n-2})(a_n q_{n-1} + q_{n-2})} \\ &= \frac{(r_n - a_n)(p_{n-1}q_{n-2} - p_{n-2}q_{n-1})}{(q_{n-1}r_n + q_{n-2})(a_n q_{n-1} + q_{n-2})}. \end{aligned}$$

Ocijenimo sada dobiveni izraz odozgo po apsolutnoj vrijednosti. Definirali smo a_n kao $\lfloor r_n \rfloor$, pa vrijedi $0 < r_n - a_n < 1$ ($0 < r_n - a_n$ vrijedi jer pretpostavljamo da postupak ne staje, odnosno, r_n nije cijeli broj). Također, iz Leme 2.1.13 slijedi da je $|p_{n-1}q_{n-2} - p_{n-2}q_{n-1}| = 1$. Budući da je $r_n > a_n$, $q_{n-1} > 0$ i prema Teoremu 2.1.11 vrijedi $q_n = a_n q_{n-1} + q_{n-2}$, imamo $r_n q_{n-1} + q_{n-2} > a_n q_{n-1} + q_{n-2} = q_n$, $n \in \mathbb{N}$. Iz navedenoga zaključujemo da vrijedi

$$|x - x_n| < \frac{1}{(q_{n-1}r_n + q_{n-2})(a_n q_{n-1} + q_{n-2})} < \frac{1}{q_n^2}.$$

Kao što smo već komentirali, q_n je strogo rastući niz za $n > 1$, pa $q_n \longrightarrow \infty$ kad $n \longrightarrow \infty$, stoga $|x - x_n| \longrightarrow 0$ kad $n \longrightarrow \infty$, pa $x_n \longrightarrow x$. Dakle, konvergente beskonačnog verižnog razlomka konvergiraju realnom broju x. □

2.2 Konstrukcija Cantorovog skupa

Ovo potpoglavlje napisano je prema [6].
Neka $S(k)$, $k \in \mathbb{Z}$, $k \geq 2$, označava skup realnih brojeva α takvih da $0 \leq \alpha \leq k^{-1}$ i razvoj broja α u verižni razlomak ne sadrži parcijalni kvocijent manji od k (nulu uzimamo kao recipročnu vrijednost beskonačnog parcijalnog kvocijenta, pa ona pripada skupu $S(k)$).
Pokazat ćemo da je za svaki $k \in \mathbb{Z}$, $k \geq 2$, skup $S(k)$ Cantorov skup točaka na intervalu $[0, k^{-1}]$.

Prisjetimo se da se Cantorov ternarni skup dobiva uklanjanjem odgovarajućeg beskonačnog skupa disjunktnih otvorenih srednjih intervala (trećina) sljedećim postupkom:

Uzmemo zatvoreni interval $A = [x, x + a]$ na realnom pravcu kojem uklanjamo srednji otvoreni interval $A_{12} = \langle x + a_1, x + a_1 + a_{12} \rangle$, $a_1, a_{12} > 0$ i $a_1 + a_{12} < a$. Preostaju dva zatvorena intervala $A_1 = [x, x + a_1]$ i $A_2 = [x + a_1 + a_{12}, x + a]$. Sada, ukoliko iz A_1 i iz A_2 na isti način uklonimo srednje otvorene intervale i isti postupak ponovimo sa svim zatvorenim intervalima koje dobijemo u svakom pojedinom koraku, tada će točke koje preostaju u skupu A (odnosno ne nalaze se niti u jednom od uklonjenih otvorenih intervala) sačinjavati Cantorov skup točaka, $C(A)$.

Na početku postupka uzmimo interval $A = [0, k^{-1}]$. Neka je $[0 : a_1, a_2, a_3, \ldots]$ verižni razlomak s parcijalnim kvocijentima a_i, $i \in \mathbb{N}$. U određivanju podintervala skupa A dva su tipa intervala s racionalnim rubnim točkama koje je potrebno razmotriti:

- *1. tip:* interval oblika *1*:

$$[[0 : a_1, a_2, a_3, \ldots, a_n], [0 : a_1, a_2, a_3, \ldots, a_{n+1}]], \tag{2.11}$$

  gdje je $n \in \mathbb{Z}$, paran i $a_i \geq k$, za svaki i.

- *2. tip:* interval oblika *2*:

$$[[0 : a_1, a_2, a_3, \ldots, a_n], [0 : a_1, a_2, a_3, \ldots, a_{n-1}]], \tag{2.12}$$

gdje je $n \in \mathbb{Z}$, paran i $a_i \geq k$, za svaki i.

Uočimo, interval od kojeg krećemo $A = [0, k^{-1}] = [[0 :], [0 : k]]$, pa je to interval oblika *1*, uz $n = 0$.
U postupku uklanjanja srednjih intervala iz svakog se intervala oblika *1* uklanja otvoreni interval oblika

$$\langle [0 : a_1, a_2, a_3, \ldots a_n, a_{n+1} + 1], [0 : a_1, a_2, a_3, \ldots, a_{n+1}, k] \rangle, \tag{2.13}$$

dok se iz svakog intervala oblika *2* uklanja otvoreni interval oblika

$$\langle [0 : a_1, a_2, a_3, \ldots, a_n, k], [0 : a_1, a_2, a_3, \ldots, a_{n-1}, a_n + 1] \rangle. \tag{2.14}$$

Uzmimo interval oblika *1* te iz njega uklonimo srednji otvoreni interval (2.13). Na lijevoj strani dobivamo

$$[[0 : a_1, a_2, a_3, \ldots, a_{n-1}, a_n], [0 : a_1, a_2, a_3, \ldots a_n, a_{n+1} + 1]], \tag{2.15}$$

što je ponovno interval oblika *1*. Na desnoj strani dobivamo

$$[[0 : a_1, a_2, a_3, \ldots, a_{n+1}, k], [0 : a_1, a_2, a_3, \ldots, a_n, a_{n+1}]], \tag{2.16}$$

što je interval oblika *2*. Uzmimo sada interval oblika *2* te promotrimo što dobivamo uklanjanjem srednjeg otvorenog intervala (2.14). Na lijevoj strani ostaje

$$[[0 : a_1, a_2, a_3, \ldots, a_n], [0 : a_1, a_2, a_3, \ldots, a_n, k]], \tag{2.17}$$

što je interval oblika *1*, dok na desnoj strane ostaje

$$[[0 : a_1, a_2, a_3, \ldots, a_{n-1}, a_n + 1], [0 : a_1, a_2, a_3, \ldots, a_{n-1}]], \tag{2.18}$$

što je interval oblika *2*. U oba slučaja uklanjanjem srednjeg otvorenog intervala dobit će se se interval oblika *1* na lijevoj strani i interval oblika *2* na desnoj strani. Ponavljanjem postupka rezultirajući Cantorov skup točaka bit će $S(k)$.
Doista, iz odabira početnog intervala, $A = [0, k^{-1}]$, $k \geq 2$, proizlazi da je za svaki $\alpha \in S(k), 0 \leq \alpha \leq k^{-1}$. Provjerimo još da uklonjeni intervali (2.13) i (2.14) ne sadrže elemente skupa $S(k)$ i da je svaki element skupa A koji se ne nalazi u $S(k)$ sadržan u nekom od uklonjenih otvorenih intervala.

Promotrimo dva tipa otvorenih intervala koje uklanjamo. Interval oblika (2.13) možemo zapisati kao $\langle[0 : a_1, a_2, a_3, \ldots, a_{n+1}, 1], [0 : a_1, a_2, a_3, \ldots, a_{n+1}, k]\rangle$. Vidimo da za $(n + 2)$. (neparni po redu) parcijalni kvocijent a_{n+2} svakog pojedinog elementa intervala vrijedi $1 < a_{n+2} < k$. Analogno, otvoreni interval oblika (2.14) koji uklanjamo možemo zapisati kao $\langle[0 : a_1, a_2, a_3, \ldots, a_n, k], [0 : a_1, a_2, a_3, \ldots, a_{n-1}, a_n, 1]\rangle$, te za $(n + 1)$. (parni po redu) parcijalni kvocijent a_{n+1} svakog pojedinog elementa intervala vrijedi $k > a_{n+1} > 1$. Zaključujemo da, povećavanjem $n \in \mathbb{N}$, uklanjamo točno one elemente koji imaju neki parcijalni kvocijent manji od k.

Marshall Hall je u [6] objavio zanimljivu primjenu konstrukcije Cantorovog skupa pomoću verižnih razlomaka. Neka su $U, V \subseteq \mathbb{R}$. Definiramo zbroj $U + V$ dva skupa točaka U i V s

$$U + V := \{u + v : u \in U,\ v \in V\}.$$

Neka su $C(A)$ i $C(B)$ dva Cantorova skupa točaka dobivena od intervala A, odnosno B, na gore opisani način. Hall je dokazao lemu koja daje dovoljan uvjet da skup $C(A) + C(B)$ pokrije cijeli interval $A + B$. Slijedi iskaz bez dokaza.

Lema 2.2.1 ([6])**.** *Neka su A, B dva intervala na skupu $\mathbb{R}$. Neka je, bez smanjenja općenitosti, duljina intervala A veća ili jednaka od duljine intervala B. Neka je omjer duljina duljeg intervala A i kraćeg intervala B manji ili jednak 3. Nadalje, pretpostavimo da je u gornjem postupku dobivanja skupova $C(A)$ i $C(B)$ duljina oba uklonjena intervala u svakom koraku manja ili jednaka od duljine preostalog zatvorenog intervala. Tada $C(A) + C(B)$ pokriva cijeli interval $A + B$.*

Ovu Lemu Hall koristi kako bi dokazao da vrijedi $S(2) + S(2) = [0, 1]$, a time i tvrdnju da se svaki realni broj može prikazati kao *zbroj* dva realna broja od kojih svaki ima racionalni dio čiji razvoj u verižni razlomak ne sadrži parcijalni kvocijent manji od 2.

Naime, koristeći Lemu 2.2.1 pokažimo da vrijedi $S(2) + S(2) = [0, 1]$. Stavimo $k = 2$ i interval $A = B := [0, k^{-1}] = [0, 2^{-1}]$. Prvo, očito je duljina intervala A jednaka duljini intervala B, pa je i veća ili jednaka, a omjer njihovih duljina manji ili jednak 3. Izračunajmo sada duljinu intervala (2.11).
Vrijedi:

$$\begin{aligned}|[[0 : a_1, a_2, a_3, \ldots, a_n], [0 : a_1, a_2, a_3, \ldots, a_{n+1}]]| &= \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\frac{p_{n+1}q_n - p_nq_{n+1}}{q_nq_{n+1}}\right| \\ &= \frac{|p_{n+1}q_n - p_nq_{n+1}|}{|q_nq_{n+1}|},\end{aligned}$$

gdje su (p_i), (q_i) nizovi definirani kao u Teoremu 2.1.11.
Sada je prema Lemi 2.1.13 brojnik jednak 1, pa je duljina intervala (2.11) jednaka

$$\frac{1}{q_n q_{n+1}}.$$

Sličnim računanjem duljine uklonjenog intervala (2.13) i duljine preostalih intervala (2.15) i (2.16) dobivamo da omjer duljina uklonjenog intervala i intervala preostalog na lijevoj strani te omjer duljine uklonjenog intervala i intervala preostalog na desnoj strani respektivno:

$$\frac{(k-1)q_n}{kq_{n+1}+q_n} \tag{2.19}$$

i

$$\frac{(k-1)q_{n+1}}{q_{n+1}+q_n}. \tag{2.20}$$

Slično, duljina intervala (2.12) je

$$\frac{1}{q_{n-1}q_n},$$

a omjer duljina uklonjenog intervala (2.14) i preostalog intervala na lijevoj strani (2.17) te omjer duljina uklonjenog intervala (2.14) i preostalog intervala na lijevoj strani (2.18) respektivno:

$$\frac{(k-1)q_n}{q_n+q_{n-1}} \tag{2.21}$$

i

$$\frac{(k-1)q_{n-1}}{kq_n+q_{n-1}}. \tag{2.22}$$

Sada, za $k = 2$, očito je (2.19), (2.20), (2.21) i (2.22) manje ili jednako 1, pa možemo primijeniti Lemu 2.2.1.

Za $k = 2$ i interval $A = B := [0, k^{-1}] = [0, 2^{-1}]$, $S(2)$ je $C(A)$. Prema prethodnoj konstrukciji vrijedi da je $C(A) = S(2)$. Sada je prema Lemi 2.2.1 $S(2) + S(2) = A + A = [0, 1]$.

Poglavlje 3

p-adski brojevi i Cantorov skup

U ovom poglavlju predstavljena su dva pristupa p-adskim brojevima, pristup sa stajališta analize i pristup sa stajališta algebre. U nastavku će biti pokazana primjena p-adskih brojeva u proučavanju nekih zanimljivih svojstava Cantorovog skupa kao što je postojanje homeomorfizma između Cantorovog skupa i skupa $\mathbb{Z}_2$ opisanog u nastavku. Poglavlje započinjemo osnovnim definicijama koje će nam koristiti u nastavku.

Definicija 3.0.1 (Grupa, [17])**.** *Neka je G neprazan skup i $*$ operacija na G. Kažemo da je G* grupa *s operacijom $*$, te označavamo uređenim parom $(G, *)$, ako vrijedi:*

(i) *G je zatvoren s obzirom na $*$, odnosno, ako su $a, b \in G$, onda je $a * b \in G$. Kažemo i da je $*$* binarna *operacija na G.*

(ii) *Postoji neutralni element, odnosno postoji $e \in G$ takav da, za svaki $a \in G$, vrijedi*

$$a * e = e * a = a.$$

(iii) *Za svaki $a \in G$ postoji $a^{-1} \in G$ takav da*

$$a * a^{-1} = a^{-1} * a = e.$$

(iv) *Operacija $*$ je asocijativna, tj. za svaki $a, b, c \in G$ vrijedi*

$$a * (b * c) = (a * b) * c.$$

Dodatno, ako je operacija $*$ komutativna, tj. ako za svaki $a, b \in G$ vrijedi

$$a * b = b * a,$$

onda kažemo da je $(G, *)$ Abelova *ili* komutativna grupa.

Definicija 3.0.2 (Prsten, [17])**.** *Neprazan skup R nazivamo* prstenom *ako su na njemu definirane dvije binarne relacije + i ∗ koje zadovoljavaju:*

(i) $a + b = b + a$, *za svaki* $a, b \in R$. *(Komutativnost zbrajanja).*

(ii) $a + (b + c) = (a + b) + c$, *za svaki* $a, b, c \in R$. *(Asocijativnost zbrajanja).*

(iii) *Postoji* $0 \in R$ *takav da* $a + 0 = 0 + a = a$, *za svaki* $a \in R$. *(Neutralni element za zbrajanje).*

(iv) *Za svaki* $a \in R$ *postoji* $-a \in R$ *takav da* $a + (-a) = (-a) + a = 0$. *(Suprotni element za zbrajanje).*

(v) $a * (b * c) = (a * b) * c$, *za svaki* $a, b, c \in R$. *(Asocijativnost množenja).*

(vi) *Vrijedi svojstvo distributivnosti, odnosno, za svaki* $a, b, c \in R$, *vrijedi:*

$$a * (b + c) = a * b + a * c$$

i

$$(b + c) * a = b * a + c * a.$$

Primijetimo da se u definiciji ne zahtijeva postojanje multiplikativnog jediničnog elementa niti komutativnost operacije $*$. Ako u prstenu R postoji jedinični element takav da za svaki $a \in R$ vrijedi $a * 1 = 1 * a = a$, onda takav prsten zovemo *prsten s jedinicom*. Također, ako za svaki $a, b \in R$ vrijedi $a * b = b * a$, onda kažemo da je R *komutativni prsten*.

Definicija 3.0.3 ([17])**.** *Prsten R s jedinicom zovemo* prsten s dijeljenjem *ako za svaki* $a \neq 0 \in R$ *postoji* $b \in R$ *takav da* $a * b = b * a = 1$. *Obično, b označavamo kao* a^{-1} *i zovemo* inverznim elementom od a s obzirom na operaciju $*$.

Primjer 3.0.4. *Prsten racionalnih brojeva* $\mathbb{Q}$ *sa standardnim operacijama zbrajanja i oduzimanja je prsten s dijeljenjem. Prsten cijelih brojeva* $\mathbb{Z}$ *nije prsten s dijeljenjem jer npr. za cijeli broj* 5 *ne postoji* $x \in \mathbb{Z}$ *takav da je* $5 * x = x * 5 = 1$.

Definicija 3.0.5 ([17]). *Za prsten R kažemo da je* polje *ako je R komutativan prsten s dijeljenjem.*

Primjer 3.0.6. *Prsten $\mathbb{C}$ kompleksnih brojeva, s uobičajenim operacijama zbrajanja i množenja, je polje. Polje kompleksnih brojeva sadrži potpolje racionalnih brojeva $\mathbb{Q} = \left\{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\right\}$.*

3.1 *p*-adski brojevi

Definicija 3.1.1 (Metrika, [8]). *Neka je $S \neq \emptyset$. Kažemo da je preslikavanje $d : S \times S \to \mathbb{R}$* metrika *ili* funkcija udaljenosti *na skupu S ako vrijedi:*

(i) $d(x, y) \geq 0$, *za svaki* $x, y \in S$,

(ii) $d(x, y) = 0$ *ako i samo ako je* $x = y$,

(iii) $d(x, y) = d(y, x)$, *za svaki* $x, y \in S$,

(iv) $d(x, y) \leq d(x, z) + d(z, y)$, *za svaki* $x, y, z \in S$.

Uređeni par (S, d) nazivamo metrički prostor, *a uvjete (i) - (iv) aksiomi metrike.*

Definicija 3.1.2 (Ultrametrika, [17]). *Neka je na nepraznom skupu S definirana funkcija $d : S \times S \to [0, \infty\rangle$. Kažemo da je d* ultrametrika *ako vrijedi:*

(i) $d(x, y) \geq 0$, *za svaki* $x, y \in S$,

(ii) $d(x, y) = 0$ *ako i samo ako je* $x = y$,

(iii) $d(x, y) = d(y, x)$, *za svaki* $x, y \in S$,

(iv) $d(x, y) \leq max\{d(x, z), d(z, y)\}$, *za svaki* $x, y, z \in S$.

Definicija 3.1.3 (Norma na polju, [17]). *Neka je F polje. Kažemo da je preslikavanje $\|\cdot\| : F \to [0, \infty\rangle$,* norma *na polju F ako vrijedi:*

(i) $\|x\| \geq 0$, *gdje je* $\|x\| = 0$ *ako i samo ako je* $x = 0$, *za svaki* $x \in F$,

(ii) $\|x \cdot y\| = \|x\| \cdot \|y\|$, *za svaki* $x, y \in F$,

(iii) $\|x + y\| \leq \|x\| + \|y\|$, *za svaki* $x, y \in F$. *(Nejednakost trokuta).*

Za normu kažemo da je *nearhimedska norma* ako nejednakost trokuta možemo zamijeniti jačim uvjetom, tj. *jakom nejednakošću trokuta*, odnosno *nejednakošću ultrametrike*:

$$\|x + y\| \leq \max\{\|x\|, \|y\|\}.$$

Ukoliko nejednakost ultrametrike ne vrijedi, normu zovemo *arhimedska norma*.

Definicija 3.1.4 (p-adska valuacija, [3])**.** *Neka je $x \in \mathbb{Z}$, $x \neq 0$ i p prost broj, $p \geq 2$. Definiramo* p-adski red *ili* p-adsku valuaciju *cijelog broja x kao:*

$$\mathrm{ord}_p x = \max\{r \in \mathbb{Z} : p^r \text{ dijeli } x\}.$$

Nadalje, za $x \in \mathbb{Q}$, p-adska valuacija definira se kao:

$$\mathrm{ord}_p x := \mathrm{ord}_p a - \mathrm{ord}_p b,$$

gdje je $x = \frac{a}{b}$ bilo koji zapis racionalnog broja, $a \in \mathbb{Z}$, $b \in \mathbb{N}$.

Primijetimo da je ord_p u gornjoj definiciji dobro definiran za racionalni broj $\frac{a}{b}$, tj. ako je $\frac{a}{b} = \frac{a'}{b'}$, onda je

$$\mathrm{ord}_p a - \mathrm{ord}_p b = \mathrm{ord}_p a' - \mathrm{ord}_p b'.$$

Neka je $x = \mathrm{ord}_p \frac{a}{b}$. Tada je za $\frac{a'}{b'} = \frac{a}{b}$ i $\mathrm{ord}_p \frac{a'}{b'} = x$. Označimo: $u := \mathrm{ord}_p a$ i $v := \mathrm{ord}_p b$. Sada je po definiciji $\mathrm{ord}_p a - \mathrm{ord}_p b = u - v = \mathrm{ord}_p \frac{a}{b} = \mathrm{ord}_p \frac{a'}{b'} = \mathrm{ord}_p a' - \mathrm{ord}_p b'$.

Napomena 3.1.5. *Dogovorno uzimamo da je* $\mathrm{ord}_p 0 = +\infty$.

Primjer 3.1.6. $\mathrm{ord}_2 96 = 5$, *jer* $2^5 \mid 96$.

Primjer 3.1.7. $\mathrm{ord}_3 \frac{7}{12} = \mathrm{ord}_3 7 - \mathrm{ord}_3 12 = 0 - 1 = -1$.

Napomena 3.1.8. *Primijetimo da je, za dani prosti broj p, svaki broj $x \in \mathbb{Q}$ moguće na jedinstven način zapisati u obliku*

$$x = p^n \frac{a}{b}, \tag{3.1}$$

gdje je $n \in \mathbb{Z}$, $p \nmid a$, $p \nmid b$ i a, b su relativno prosti.

Propozicija 3.1.9 ([3])**.** *Za $x \in \mathbb{Q}$ vrijedi $\mathrm{ord}_p x = n$ ako i samo ako je $x = p^n \frac{a}{b}$, gdje su a i b relativno prosti te $p \nmid a$, $p \nmid b$, $n \in \mathbb{Z}$.*

Dokaz. Pokažimo prvo smjer ($\Longleftarrow$).
Neka je

$$x = \frac{p^n a}{b}.$$

Iz definicije valuacije za $x \in \mathbb{Q}$ imamo

$$\mathrm{ord}_p x = \mathrm{ord}_p \left(\frac{p^n a}{b} \right) = \mathrm{ord}_p \left(p^n a \right) - \mathrm{ord}_p \left(b \right).$$

Sada, zbog uvjeta da $p \nmid a$ i $p \nmid b$ slijedi

$$\mathrm{ord}_p \left(p^n a \right) - \mathrm{ord}_p \left(b \right) = n - 0 = n.$$

Pokažimo sada smjer ($\Longrightarrow$).
Neka je za racionalni broj $x = \frac{c}{d}$, $c \in \mathbb{Z}, d \in \mathbb{N}$,

$$\mathrm{ord}_p x = n.$$

Tada je,

$$\mathrm{ord}_p c - \mathrm{ord}_p d = n.$$

Označimo $\mathrm{ord}_p c = z$ i $\mathrm{ord}_p d = w$, gdje su $z, w \in \mathbb{N}_0$. Tada postoje $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ takvi da $c = p^z a$ i $d = p^w b$ i vrijedi

$$z - w = n. \tag{3.2}$$

Sada, zbog (3.2), x možemo zapisati kao

$$x = \frac{c}{d} = \frac{p^z a}{p^w b} = p^n \frac{a}{b},$$

pri čemu skratimo a i b tako da budu relativno prosti.
Time je tvrdnja dokazana. □

Propozicija 3.1.10 ([3])**.** *Neka su x,y* $\in \mathbb{Q}$ *i p prost broj. Valuacija* ord_p *ima sljedeća svojstva:*

(i) $\mathrm{ord}_p x = +\infty$ *ako i samo ako je* $x = 0$,

(ii) $\mathrm{ord}_p(xy) = \mathrm{ord}_p x + \mathrm{ord}_p y$,

(iii) $\mathrm{ord}_p(x+y) \geq \min\{\mathrm{ord}_p x, \mathrm{ord}_p y\}$, *pri čemu jednakost vrijedi ako i samo ako je* $\mathrm{ord}_p x \neq \mathrm{ord}_p y$.

Dokaz. (i) Očito je $\mathrm{ord}_p x = \max\{r : p^r \mid x\} = \infty$ ako i samo ako $p^\infty \mid x$ ako i samo ako $x = 0$.
U dokazu (ii) i (iii) koristimo sljedeće:
Neka su $x = p^u \frac{a}{b}$ i $y = p^v \frac{c}{d}$, $u, v \in \mathbb{N}_0$, takvi da $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$ i $p \nmid a, b, c, d$ tj. $\mathrm{ord}_p x = u$ i $\mathrm{ord}_p y = v$.
(ii) Tada je $xy = p^{u+v} \frac{ac}{bd}$, gdje $p \nmid ac, bd$, iz čega slijedi

$$\mathrm{ord}_p(xy) = u + v = \mathrm{ord}_p x + \mathrm{ord}_p y.$$

(iii) Bez smanjenja općenitosti možemo pretpostaviti da je $u \leq v$. Tada je

$$x + y = p^u \left(\frac{a}{b} + p^{v-u} \frac{c}{d} \right).$$

1° Ako je $u = v$, tada je $\mathrm{ord}_p(x + y) \geq u = \min\left\{\mathrm{ord}_p x, \mathrm{ord}_p y\right\}$.
2° $u \neq v$, onda je

$$x + y = p^u \left(\frac{ad + p^{v-u} bc}{bd} \right).$$

Kako $p \nmid ad$ i $v - u > 0$, imamo da je

$$\mathrm{ord}_p(x + y) = u = \min\left\{\mathrm{ord}_p x, \mathrm{ord}_p y\right\}.$$

□

Definicija 3.1.11 (p-adska norma, [3])**.** . *Za $x \in \mathbb{Q}$ i $p \in \mathbb{N}$ prost, definiramo* p-adsku normu *racionalnog broja x s*

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p x}, & \text{za } x \neq 0, \\ p^{-\infty} = 0, & \text{za } x = 0. \end{cases} \tag{3.3}$$

Propozicija 3.1.12 ([3])**.** *Za $p \in \mathbb{N}$ prost, funkcija $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$ ima sljedeća svojstva:*

(i) $|x|_p = 0$ *ako i samo ako je $x = 0$, za svaki $x \in \mathbb{Q}$,*

(ii) $|xy|_p = |x|_p |y|_p$*, za svaki $x, y \in \mathbb{Q}$,*

(iii) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$*, uz jednakost ako i samo ako je $|x|_p \neq |y|_p$, za svaki $x, y \in \mathbb{Q}$.*

Dokaz. Za svaki $s \in \mathbb{R}$ vrijedi $\frac{1}{p^s} > 0$, pa (i) očito slijedi iz Definicije 3.1.11. Dokažimo (ii). Za $x = 0$ ili $y = 0$ iz definicije p-adske norme slijedi da je $|x|_p = 0$ ili $|y|_p = 0$ i $|xy|_p = |0|_p = 0$, pa tvrdnja očito vrijedi. Neka su sada $x, y \in \mathbb{Q}$ različiti od nule. Tada je

$$|xy|_p = \frac{1}{p^{\mathrm{ord}_p(xy)}} = \frac{1}{p^{\mathrm{ord}_p x + \mathrm{ord}_p y}} = \frac{1}{p^{\mathrm{ord}_p x} p^{\mathrm{ord}_p y}} = |x|_p |y|_p.$$

Preostaje dokazati (iii). Za $x = 0$, $y = 0$ ili $x + y = 0$ dokaz je trivijalan, stoga, neka su $x, y \in \mathbb{Q}$ različiti od nule. Iz $\mathrm{ord}_p(x + y) \geq \min\{\mathrm{ord}_p x, \mathrm{ord}_p y\}$ (Propozicija 3.1.10), slijedi da je i $p^{\mathrm{ord}_p(x+y)} \geq \min\{p^{\mathrm{ord}_p x}, p^{\mathrm{ord}_p y}\}$, pa je $p^{-\mathrm{ord}_p(x+y)} \leq \max\{p^{-\mathrm{ord}_p x}, p^{-\mathrm{ord}_p y}\}$. Iz Definicije 3.1.11 sada imamo

$$|x + y|_p = p^{-\mathrm{ord}_p(x+y)} \leq \max\{p^{-\mathrm{ord}_p x}, p^{-\mathrm{ord}_p y}\} = \max\{|x|_p, |y|_p\}.$$

□

Iz svojstva (iii) Propozicije 3.1.12 vidimo da je $|\cdot|_p$ nearhimedska norma na $\mathbb{Q}$.

Definicija 3.1.13 (p-adska udaljenost, [17])**.** *Neka su $x, y \in \mathbb{Q}$ i p prost broj. Definiramo* p-adsku udaljenost *između x i y s*

$$d_p(x, y) = |x - y|_p.$$

Dokažimo da je, s tako definiranom udaljenošću, uređeni par $(\mathbb{Q}, d_p)$ metrički prostor. Preuzeto iz [17]. Iz definicije p-adske norme je $|x-y|_p \geq 0$, za svaki $x, y \in \mathbb{Q}$, te $|x-y|_p = 0$ ako i samo ako je $x = y$, pa svojstva (i) i (ii) iz Definicije 3.1.1, očito vrijede. Dokažimo (iii). Primijetimo da je $|-1|_p = p^{-\mathrm{ord}_p(-1)} = p^0 = 1$. Za svaki $x, y \in \mathbb{Q}$ vrijedi

$$d_p(x, y) = |x - y|_p = |-1(y - x)|_p = |-1|_p |y - x|_p = |y - x|_p = d(y - x)_p.$$

Preostaje pokazati (iv). Za svaki $x, y, z \in \mathbb{Q}$ vrijedi

$$\begin{aligned} d(x, y)_p &= |x - y|_p = |x - z + z - y|_p \leq max\{|x - z|_p, |z - y|_p\} \leq |x - z|_p + |z - y|_p \\ &= d(x, z)_p + d(z, y)_p. \end{aligned}$$

Pokazali smo da p-adska udaljenost zadovoljava svojstva metrike. Štoviše, pokazali smo da p-adska udaljenost ima jača svojstva nego metrika. Ona zadovoljava svojstva ultrametrike.

Prisjetimo se da polje $\mathbb{Q}$ nije potpuno u odnosu na standardnu (arhimedsku) normu $|\cdot|$, gdje $|\cdot|$ predstavlja apsolutnu vrijednost broja. Sljedeći primjer pokazuje da polje $\mathbb{Q}$ nije

potpuno ni u odnosu na normu $|\cdot|_p$, $p \in \mathbb{N}$ prost. Prije samog primjera prisjetimo se pojma kongruencije i Eulerovog teorema kojeg navodimo bez dokaza.
Za $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$ definiramo relaciju $\equiv \pmod{n}$ kongruencije modulo n na $\mathbb{Z}$ na sljedeći način: a je kongruentno b modulo n ako i samo ako $n \mid (b-a)$.
Pišemo, $a \equiv b \pmod{n}$.

Teorem 3.1.14 (Eulerov teorem, [1]). *Neka su $a, n \in \mathbb{N}$ relativno prosti brojevi. Tada je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \tag{3.4}$$

gdje je $\varphi(n)$ broj definiran s $\varphi(n) = \operatorname{card}(\{x \in \mathbb{Z} : 1 \leq x \leq n, (x,n) = 1\})$.

Pokažimo u Primjeru 3.1.16 da normirani prostor $(\mathbb{Q}, |\cdot|_p)$ nije potpun vektorski prostor. Pokazat ćemo za $p > 3$. Tvrdnja je istinita i za $p = 2, 3$, ali nećemo navoditi kontraprimjer. Dakle, u primjeru ćemo pronaći niz racionalnih brojeva koji je Cauchyjev u normi $|\cdot|_p$, ali u toj normi ne konvergira.
Prije samog primjera, trebat će nam definicija Cauchyjevog niza u normiranom prostoru.

Definicija 3.1.15 ([16]). *Kažemo da je niz $(x_n)_{n\in\mathbb{N}}$ u normiranom prostoru $(X, |\cdot|)$* Cauchyjev niz *ako za svaki $\epsilon > 0$ postoji $n_\epsilon \in \mathbb{N}$ takav da za sve $n, m \in \mathbb{N}$, $n, m \geq n_\epsilon$, vrijedi*

$$|x_n - x_m| < \epsilon.$$

Primjer 3.1.16 ([16]). *Neka je $p > 3$ prost broj. Uzmimo $a \in \mathbb{Z}$ takav da $1 < a < p-1$. Označimo s $(x_n)_n \in \mathbb{N}$ niz racionalnih brojeva, gdje je $x_n := a^{p^n}$, $n \in \mathbb{N}$. Provjerimo da je ovo Cauchyjev niz:*

$$x_{n+1} - x_n = a^{p^{n+1}} - a^{p^n} = a^{p^n}(a^{p^n(p-1)} - 1).$$

Iz Eulerovog teorema slijedi da je $a^{p^n(p-1)} - 1 \equiv 0 \pmod{p^{n+1}}$, jer je $\varphi(p^{n+1}) = p^{n+1} - p^n = p^n(p-1)$. Sada, iz definicije p-adske udaljenosti i iz svojstava p-adske norme slijedi

$$|x_{n+1} - x_n|_p = \left|a^{p^n}(a^{p^n(p-1)} - 1)\right|_p = \left|a^{p^n}\right|_p \left|a^{p^n(p-1)} - 1\right|_p < p^0 \cdot p^{-n} = p^{-n},$$

a $p^{-n} \longrightarrow 0$, kad $n \longrightarrow \infty$, pa je $(x_n)_n \in \mathbb{N}$ Cauchyjev niz u $(\mathbb{Q}, |\cdot|_p)$.
Pretpostavimo sada da $(x_n)_{n\in\mathbb{N}}$ konvergira, u p-adskoj normi, nekom broju $x \in \mathbb{Q}$, tj. $x = \lim_{n\to\infty} x_n$. Primijetimo da $|x - x_n|_p \to 0$ kad $n \to \infty$ povlači

$$\lim_{n\to\infty} |x_n|_p = |x|_p.$$

Kako za svaki $n \in \mathbb{N}$ vrijedi da $p \nmid a^{p^n} = x_n$, slijedi da je $\operatorname{ord}_p x_n = 0$, za svaki $n \in \mathbb{N}$, pa je $|x|_p = \lim_{n\to\infty} |x_n|_p = 1$.

Iz svojstava p-adske norme slijedi da je $x \neq 0$*. S druge strane, imamo*

$$x = \lim_{n\to\infty} x_n = \lim_{n\to\infty} x_{n+1} = \lim_{n\to\infty} (x_n)^p = \left(\lim_{n\to\infty} x_n\right)^p = x^p.$$

Sada je, zbog $x \neq 0$*,* $x^{p-1} = 1$*, iz čega slijedi* $x = 1$ *ili* $x = -1$*. Stoga je* $a - x$ *cijeli broj i* $0 < a - x < p$*. Zaključujemo da* $p \nmid (a - x)$*, pa je, opet kao i gore,* $|x - a|_p = 1$*.*
Kako $x_n \to x$ *kad* $n \to \infty$*, postoji* $N \in \mathbb{N}$ *takav da za svaki* $n \in \mathbb{N}, n > N$*, vrijedi:*

$$|x_n - x|_p < |x - a|_p = 1,$$

odnosno,

$$\left|a^{p^n} - x\right|_p < |x - a|_p . \tag{3.5}$$

Za takve $n > N$*, s druge strane također vrijedi*

$$|x - a|_p = \left|x - a^{p^n} + a^{p^n} - a\right|_p \leq \max\{\left|x - a^{p^n}\right|_p, \left|a^{p^n} - a\right|_p\}, \tag{3.6}$$

prema svojstvima ultrametrike.
Kako je, prema (3.5)*,* $\left|x - a^{p^n}\right|_p < |x - a|_p$*, iz* (3.6) *zaključujemo da je*

$$|x - a|_p = \left|a^{p^n} - a\right|_p = |a|_p \left|a^{p^n-1} - 1\right|_p = \left|a^{p^n-1} - 1\right|_p < 1,$$

pri čemu posljednja nejednakost slijedi iz Korolara[2] *koji slijedi iz Fermatovog malog teorema*[1] *. Dobiveni rezultat je kontradikcija s tvrdnjom da je* $|x - a|_p = 1$*. Dakle, Cauchyjev niz* $(x_n)_{n\in\mathbb{N}}$ *ne konvergira u* $(\mathbb{Q}, |\cdot|_p)$*.*

3.1.1 Upotpunjenje $(\mathbb{Q}, |\cdot|_p)$

Upotpunimo sada polje $\mathbb{Q}$ do polja koje označavamo $\mathbb{Q}_p$. Jedan od načina na koji je moguće doći do upotpunjenja polja $\mathbb{Q}$ jest koristeći Cauchyjeve nizove. Prisjetimo se upotpunjenja polja $\mathbb{Q}$ s euklidskom normom do skupa realnih brojeva, $\mathbb{R}$. Slična se ideja može primijeniti i na skup $\mathbb{Q}$ s definiranom p-adskom normom i p-adskom udaljenosti induciranom takvom normom.

---

[1] **Teorem 3.1.17** (Fermatov mali teorem, [1]). *Neka je* p *prost broj i* $a \in \mathbb{N}$ *takav da* $p \nmid a$*. Tada je* $a^{p-1} \equiv 1 \pmod{p}$*.*

[2] **Korolar 3.1.18** ([2]). *Neka je* p *prost broj te* $k \in \mathbb{Z}$*,* $k > 0$*, i neka je* $n \in \mathbb{N}$ *takav da* $p \nmid n$*. Tada je* $n^{p^k-1} \equiv 1 \pmod{p}$*.*

Definicija 3.1.19 (p-adska ekvivalencija Cauchyjevih nizova, [11])**.** *Neka je p fiksan prost broj. Za dva Cauchyjeva niza* (x_n) *i* (y_n) *u normiranom prostoru* $(\mathbb{Q}, |\cdot|_p)$*, pri čemu je* $x_n, y_n \in \mathbb{Q}$*, za svaki* $n \in \mathbb{N}$*, kažemo da su* ekvivalentna *u odnosu na p-adsku normu ako vrijedi*

$$\lim_{n\to\infty} |x_n - y_n|_p = 0.$$

Označimo s (x) konstantan Cauchyjev niz u kojemu su svi članovi jednaki x, $x \in \mathbb{Q}$. Očito je $(x) \sim (x')$ ako i samo ako je $x = x'$, $x' \in \mathbb{Q}$. Klasu ekvivalencije konstantnog niza (x) označavamo često i samo s x. Klasu ekvivalencije niza (0) tako označavamo s 0.

Dokažimo da je ekvivalencija Cauchyjevih nizova, u oznaci $\sim$, *relacija ekvivalencije*.
Neka su (x_n) i (y_n) Cauchyjevi nizovi u normiranom prostoru $(\mathbb{Q}, |\cdot|_p)$, $x_n, y_n \in \mathbb{Q}$, za svaki $n \in \mathbb{N}$. Vrijedi, $(x_n) \sim (x_n)$ jer je $(x_n - x_n)_{n\in\mathbb{N}}$ *konstantan niz* s vrijednošću 0, pa je $\lim_{n\to\infty} |x_n - x_n|_p = \lim_{n\to\infty} |0|_p = 0$ i vrijedi da je relacija $\sim$ *refleksivna*.
Neka su $(x_n), (y_n)$ nizovi takvi da je $(x_n) \sim (y_n)$, tj. $\lim_{n\to\infty} |x_n - y_n|_p = 0$. Tada je i $\lim_{n\to\infty} |-(x_n - y_n)|_p = \lim_{n\to\infty} |y_n - x_n|_p = 0$, pa vrijedi da je relacija $\sim$ *simetrična*.
Neka su $(x_n), (y_n), (z_n)$ nizovi takvi da je $(x_n) \sim (y_n)$ i $(y_n) \sim (z_n)$, tj. $\lim_{n\to\infty} |x_n - y_n|_p = 0$ i $\lim_{n\to\infty} |y_n - z_n|_p = 0$, pa je $\lim_{n\to\infty} |x_n - z_n|_p = \lim_{n\to\infty} |(x_n - y_n) + (y_n - z_n)|_p \leq \lim_{n\to\infty} \left(\max\{|x_n - y_n|_p, |y_n - z_n|_p\}\right) = 0$ i relacija $\sim$ je *tranzitivna*, pa slijedi da je *relacija ekvivalencije*. Preuzeto iz [17] i [9].

Pomoću te relacije sada možemo definirati *klase p-ekvivalentnih Cauchyjevih nizova*. Skup svih klasa ekvivalencije Cauchyjevih nizova u $(\mathbb{Q}, |\cdot|_p)$ bit će *upotpunjenje skupa* $\mathbb{Q}$, u oznaci $\mathbb{Q}_p$.

Definicija 3.1.20 (p-adska norma klase ekvivalencije Cauchyjevih nizova, [11])**.** *Neka je* $[a]$ *klasa čiji je reprezentant niz racionalnih brojeva* (a_n)*. Definiramo p-*adsku normu klase ekvivalencije $[a]$ *kao:*

$$|[a]|_p = \lim_{n\to\infty} |a_n|_p \,,$$

gdje je (a_n) bilo koji *reprezentant klase* $[a]$.

Limes u Definiciji 3.1.19 postoji jer:

- ako je $[a] = 0$, onda je $\lim_{n\to\infty} |a_n|_p = 0$, po definiciji.

- ako $[a] \neq 0$, onda postoji $\epsilon > 0$ takav da za svaki $N \in \mathbb{N}$ postoji indeks $i_N \in \mathbb{N}$, $i_N > N$, takav da vrijedi:

$$|a_{i_N}|_p > \epsilon. \tag{3.7}$$

Budući da je (a_n) po definiciji Cauchyjev niz, za $\epsilon > 0$ kao gore te za dovoljno velik N, vrijedi $|a_i - a_{i'}|_p < \epsilon$, za sve $i, i' > N$, $i, i' \in \mathbb{N}$. Stoga,

$$|a_{i_N} - a_i|_p < \epsilon, \tag{3.8}$$

za $i_N, i > N, i_N, i \in \mathbb{N}$.
Znamo da, za i_N, i kao gore, vrijedi: $|a_{i_N}|_p = |(a_{i_N} - a_i) + a_i|_p \leq \max\left\{|a_{i_N} - a_i|_p, |a_i|_p\right\}$, a kako je, zbog (3.7) i (3.8), $|a_{i_N}|_p > |a_{i_N} - a_i|_p$, mora biti $|a_{i_N}|_p \leq |a_i|_p$.
S druge strane, za i_N, i kao gore, vrijedi $|a_i|_p = |a_{i_N} + (a_i - a_{i_N})|_p \leq \max\left\{|a_{i_N}|_p, |a_i - a_{i_N}|_p\right\}$, pa je, zbog (3.7) i (3.8), $|a_i|_p \leq |a_{i_N}|_p$.
Zaključujemo da vrijedi jednakost $|a_i|_p = |a_{i_N}|_p$. Dakle, za svaki $i > N$, $|a_i|_p$ ima konstantnu vrijednost $|a_{i_N}|_p$. Tada je $\lim_{i\to\infty} |a_i|_p$ jednak toj konstanti. Preuzeto iz [11].

Također, primijetimo da definicija ne ovisi o reprezentantu jer za ekvivalentne nizove (x_n), (y_n), predstavnike klase $[a]$, vrijedi da je $\lim_{n\to\infty} |x_n - y_n|_p = 0$. Naime, iz svojstava p-adske norme slijedi:

$$|x_n|_p = |x_n - y_n + y_n|_p \leq |x_n - y_n|_p + |y_n|_p. \tag{3.9}$$

Analogno,

$$|y_n|_p = |y_n - x_n + x_n|_p \leq |y_n - x_n|_p + |x_n|_p. \tag{3.10}$$

Zbog $|y_n - x_n|_p = |(-1)(x_n - y_n)|_p = |-1|_p |x_n - y_n|_p = |x_n - y_n|_p$ i iz (3.9) i (3.10) slijedi:

$$0 \leq ||x_n|_p - |y_n|_p| \leq |x_n - y_n|_p.$$

Sada je $0 \leq \lim_{n\to\infty} ||x_n|_p - |y_n|_p| \leq \lim_{n\to\infty} |x_n - y_n|_p = 0$, pa iz Teorema o sendviču slijedi $\lim_{n\to\infty} ||x_n|_p - |y_n|_p| = 0$, tj. $\lim_{n\to\infty} |x_n|_p = \lim_{n\to\infty} |y_n|_p$. Preuzeto iz [11].

Na *prostoru klasa* $\mathbb{Q}_p$ ekvivalentnih Cauchyjevih nizova definiramo operacije *zbrajanja* i *množenja*. Umnožak klasa $[a]$ i $[b]$ definiramo kao klasu

$$[a] \cdot [b] := [a_n \cdot b_n],$$

gdje su (a_n) i (b_n) bilo koji predstavnici klasa $[a]$ i $[b]$. Pokažimo da je ta operacija dobro definirana, tj. neovisna o izboru predstavnika klasa.

Neka su (a'_n) i (b'_n) Cauchyjevi nizovi takvi da je $(a'_n) \sim (a_n)$ i $(b'_n) \sim (b_n)$. Pokažimo da vrijedi $(a'_n b'_n) \sim (a_n b_n)$. Imamo

$$\left|a'_n b'_n - a_n b_n\right|_p = \left|a'_n(b'_n - b_n) + b_n(a'_n - a_n)\right|_p \leq \max\left\{\left|a'_n(b'_n - b_n)\right|_p, \left|b_n(a'_n - a_n)\right|_p\right\}.$$

Kad $n \to \infty$ prvi izraz pod maksimumom poprima vrijednost $|[a]|_p \cdot \lim_{n\to\infty} |b'_n - b_n|_p = 0$, a drugi $|[b]|_p \cdot \lim_{n\to\infty} |a'_n - a_n|_p = 0$, pa slijedi da je $\lim_{n\to\infty} |a'_n b'_n - a_n b_n|_p = 0$, odnosno, $(a'_n b'_n) \sim (a_n b_n)$.

Na sličan način definiramo operaciju zbrajanja na klasama u $\mathbb{Q}_p$. Zbroj klasa $[a]$ i $[b]$ definiramo kao klasu

$$[a] + [b] := [a_n + b_n],$$

gdje su (a_n) i (b_n) bilo koji predstavnici klasa $[a]$ i $[b]$.
Ponovno, neka su (a'_n) i (b'_n) Cauchyjevi nizovi takvi da je $(a'_n) \sim (a_n)$ i $(b'_n) \sim (b_n)$. Pokažimo da je operacija zbrajanja dobro definirana. Vrijedi:

$$\left|(a'_n + b'_n) - (a_n + b_n)\right|_p = \left|a'_n - a_n + b'_n - b_n\right|_p \leq \max\left\{\left|a'_n - a_n\right|_p, \left|b'_n - b_n\right|_p\right\}.$$

Sada iz $(a'_n) \sim (a_n)$ i $(b'_n) \sim (b_n)$ slijedi da je $\lim_{n\to\infty} |a'_n - a_n|_p = 0$ i $\lim_{n\to\infty} |b'_n - b_n|_p = 0$. Zaključujemo da je $\lim_{n\to\infty} \left(|(a'_n + b'_n) - (a_n + b_n)|_p\right) = 0$, odnosno $(a'_n + b'_n) \sim (a_n + b_n)$. Preuzeto iz [11].

Propozicija 3.1.21 ([11])**.** *Skup klasa ekvivalencije Cauchyjevih nizova racionalnih brojeva, $\mathbb{Q}_p$, uz gore definirane operacije zbrajanja i množenja, je polje.*

Dokaz. Neka su $[a], [b], [c] \in \mathbb{Q}_p$ klase ekvivalencije s reprezentantima $(a_n), (b_n), (c_n)$ respektivno.

- Komutativnost zbrajanja: $[a] + [b]$ je klasa ekvivalencije reprezentirana nizom $(a_n + b_n) = (b_n + a_n)$. Dakle, $b + a$ je također klasa ekvivalencije, odnosno, $[a] + [b] = [b] + [a]$.
- Asocijativnost zbrajanja: $[a] + ([b] + [c])$ je klasa ekvivalencije s reprezentantom $(a_n + (b_n + c_n)) = (a_n + b_n + c_n) = ((a_n + b_n) + c_n)$, pa je i $([a] + [b]) + [c]$ klasa ekvivalencije, odnosno, $[a] + ([b] + [c]) = ([a] + [b]) + [c]$.
- Neutralni element za zbrajanje: $[a] + 0$ je klasa ekvivalencije reprezentirana nizom $(a_n + 0)$. Također, $(a_n + 0) = (a_n)$. Dakle, $[a]$ je također klasa ekvivalencije reprezentirana tim nizom. Slijedi, $0 + [a] =$ (komutativnost zbrajanja) $= [a] + 0 = [a]$, pa je 0 neutralni element za zbrajanje.

- Suprotni element za zbrajanje: Za klasu ekvivalencije $[a]$ suprotni element za zbrajanje je ona klasa ekvivalencije $[b]$ reprezentirana s $(b_n) = (-a_n)$.

- Komutativnost množenja se dokazuje analogno kao za zbrajanje.

- Asocijativnost množenja se dokazuje analogno kao za zbrajanje.

- Neutralni element za množenje: $[a] \cdot 1$ je klasa ekvivalencije reprezentirana nizom $(a_n \cdot 1)$. Također, $(a_n \cdot 1) = (a_n)$. Dakle, $[a]$ je također klasa ekvivalencije reprezentirana tim nizom. Slijedi, $1 \cdot [a] =$ (komutativnost množenja) $= [a] \cdot 1 = a$, pa je $1 \neq 0$ neutralni element za množenje.

- Inverzni element za množenje: Ukoliko za neke elemente niza (a_n) vrijedi da je $a_n = 0$, tada definiramo niz (a'_n) s

$$a'_n := \begin{cases} a_n, & a_n \neq 0, \\ p^n, & a_n = 0. \end{cases}$$

  Takav je Cauchyjev niz ekvivalentan nizu (a_n), pa inverzni element za množenje klase $[a]$ možemo definirati kao klasu $[b]$ reprezentiranu nizom $(b_n) = \left(\frac{1}{a'_n}\right) = \left(a_n^{-1}\right)$.

- Pravilo distribucije: $[a]([b] + [c])$ je klasa ekvivalencije s reprezentantom

$$(a_n(b_n + c_n)) = (a_n b_n + a_n c_n),$$

  pa je $[a][b] + [a][c]$ također klasa ekvivalencije, odnosno, $[a]([b] + [c]) = [a][b] + [b][c]$.
  Analogno, $([b] + [c])[a]$ je klasa ekvivalencije s reprezentantom

$$((b_n + c_n)a_n) = (b_n a_n + c_n a_n),$$

  pa je $[b][a] + [c][a]$ također klasa ekvivalencije, odnosno, $([b] + [c])[a] = [b][a] + [c][a]$.

Zaključujemo da je $\mathbb{Q}_p$, uz operacije zbrajanja i množenja definirane kao gore, polje. □

Definicija 3.1.22 (p-adski brojevi, [11])**.** *Polje* $(\mathbb{Q}_p, |\cdot|_p)$ *definirano kao gore zovemo* polje p-adskih brojeva*, a njegove elemente* $[a]$ *(klase ekvivalentnih Cauchyjevih nizova) nazivamo* p-adskim brojevima*.*

Propozicija 3.1.23 ([11])**.** *Polje p-adskih brojeva* $\mathbb{Q}_p$ *je potpuno u odnosu na normu* $|\cdot|_p$*.*

Dokaz. Neka je $([a_j])_j$, $j \in \mathbb{N}$, proizvoljan Cauchyjev niz klasa ekvivalencije u $\mathbb{Q}_p$. Pripadajuće reprezentante klasa $[a_j]$ označimo s $(a_{j,i})_i$. Znamo da su to Cauchyjevi nizovi racionalnih brojeva, pa vrijedi:
Za svaki $j \in \mathbb{N}$ i za svaki $\varepsilon > 0$, postoji $N_{j,\varepsilon} \in \mathbb{N}$, takav da, za sve $i, i' \geq N_{j,\varepsilon}$, vrijedi $\left|a_{j,i} - a_{j,i'}\right|_p < \varepsilon$. Posebno, za $\varepsilon = \frac{1}{p^j}$, $j \in \mathbb{N}$, postoji $N_j \in \mathbb{N}$, takav da, za sve $i, i' \geq N_j$, vrijedi

$$\left|a_{j,i} - a_{j,i'}\right|_p < \frac{1}{p^j}. \tag{3.11}$$

Provjerimo da je $(a_{j,N_j})_j$ Cauchyjev niz racionalnih brojeva. Naime, kako je $[a_j]_j$ Cauchyjev niz, za svaki $\varepsilon > 0$ postoji $j_0 \in \mathbb{N}$ takav da za svaki $i, k \geq j_0$, $i, k \in \mathbb{N}$, vrijedi:

$$\lim_{n\to\infty} |a_{i,n} - a_{k,n}|_p = |[a_i - a_k]|_p = |[a_i] - [a_k]|_p \leq \frac{\varepsilon}{3}. \tag{3.12}$$

Uzmimo sada $\varepsilon > 0$. Tada postoji $j_1 \in \mathbb{N}$ takav da $\frac{1}{p^{j_1}} < \frac{\varepsilon}{3}$. Tada za svaki $m > j_1$, $m \in \mathbb{N}$, vrijedi također $\frac{1}{p^m} < \frac{1}{p^{j_1}} < \varepsilon$.

Sada stavimo $J := \max\{j_0, j_1\}$. Za $m, n > J$, prema (3.11) i (3.12) i uz izbor dovoljno velikog $N > \max\{N_m, N_n\}$, vrijedi sljedeće:

$$\begin{aligned} |a_{m,N_m} - a_{n,N_n}| &\leq |a_{m,N_m} - a_{m,N}| + |a_{m,N} - a_{n,N}| + |a_{n,N} - a_{n,N_n}| \\ &\leq \frac{1}{p^{j_0}} + \frac{\varepsilon}{3} + \frac{1}{p^{j_0}} < \varepsilon. \end{aligned}$$

Tvrdimo da je klasa ekvivalencije niza $(a_{j,N_j})_j$, limes niza $([a_j])_j$.
Stavimo $\overline{a} := (a_{j,N_j})_j$. Pokažimo da je $[\overline{a}]$ limes niza $([a_j])_j$.

Uzmimo $\varepsilon > 0$ i uzmimo j_0 takav da je $\frac{1}{j_0} < \varepsilon$. Iz definicije p-adske norme, za $j \geq j_0$, prema (3.11) i zbog Cauchyjevosti niza (a_{j,N_j}), vrijedi:

$$\begin{aligned} |[a_j] - [\overline{a}]|_p &= \lim_{i\to\infty} |a_{j,i} - a_{i,N_i}|_p \\ &\leq \lim_{i\to\infty} |a_{j,i} - a_{j,N_j}|_p + \lim_{i\to\infty} |a_{j,N_j} - a_{i,N_i}|_p \\ &\leq \frac{\varepsilon}{3} + \frac{\varepsilon}{3} < \varepsilon. \end{aligned} \tag{3.13}$$

Slijedi, $|[a_j] - [\overline{a}]|_p \to 0$, kad $j \to \infty$, odnosno, $[a_j] \to [\overline{a}]$ u $\mathbb{Q}_p$, kad $j \to \infty$.
Dakle, svaki Cauchyjev niz u $\mathbb{Q}_p$ je konvergentan s obzirom na p-adsku normu, odnosno, polje $\mathbb{Q}_p$ je potpuno. □

3.1.2 Drugi način prikaza p-adskih brojeva: p-adska ekspanzija

U dokazu Teorema 3.1.25 koji će nam omogućiti prijelaz s apstraktnih klasa ekvivalencije Cauchyjevih nizova na konkretniji zapis elemenata $\mathbb{Q}_p$, u obliku tzv. *p-adske ekspanzije*, koristimo sljedeću lemu. Takav, operativniji zapis, koristit će nam u potpoglavlju 3.3 Primjena p-adskih brojeva u Cantorovom skupu.

Lema 3.1.24 ([11])**.** *Neka je $x \in \mathbb{Q}$ takav da je $|x|_p \leq 1$. Tada, za svaki $i \in \mathbb{N}$, postoji jedinstveni $\alpha \in \{0, 1, 2, \ldots, p^i - 1\}$ takav da vrijedi $|\alpha - x|_p \leq p^{-i}$.*

Dokaz. Neka je $x = \frac{a}{b}$, do kraja skraćen razlomak, $a \in \mathbb{Z}, b \in \mathbb{N}$. Fiksirajmo $i \in \mathbb{N}$. Kako je $|x|_p \leq 1$, mora biti $\mathrm{ord}_p x \geq 1$, tj. postoji prirodan broj $k \geq 1$ takav da $x = p^k \frac{c}{b}$ (tj. $k := \mathrm{ord}_p x$), $c \in \mathbb{Z}$, pri čemu $p \nmid b$. Zato su b i p^i relativno prosti. Prema Euklidovom algoritmu, sada postoje $m, n \in \mathbb{Z}$ takvi da je $mb + np^i = 1$.
Stavimo $\alpha = am$. Tada vrijedi:

$$|\alpha - x|_p = \left|am - \frac{a}{b}\right|_p = \left|\frac{a}{b}\right|_p |mb - 1|_p \leq |mb - 1|_p = \left|np^i\right|_p = |n|_p \left(\frac{1}{p^i}\right) \leq \frac{1}{p^i}.$$

Posljednja nejednakost vrijedi jer je za $n \in \mathbb{Z}$, $|n|_p \leq 1$. Konačno, ako $\alpha \notin \{0, 1, 2, \ldots, p^i - 1\}$, tada postoji jedinstveni $k \in \mathbb{Z}$ takav da je $\alpha + kp^i \in \{0, 1, 2, \ldots, p^i - 1\}$. Za takav α i dalje vrijedi $|\alpha + kp^i - x|_p = |\alpha - x + kp^i|_p \leq \max\{|\alpha - x|_p, |kp^i|_p\} \leq p^{-i}$. □

Teorem 3.1.25 ([11])**.** *Svaka klasa ekvivalencije $[a] \in \mathbb{Q}_p$ za koju vrijedi $|[a]|_p \leq 1$ ima točno jedan reprezentantni Cauchyjev niz cijelih brojeva $(a_i)_i$ za kojeg vrijedi:*

(i) *$a_i \in \mathbb{N}_0$, $a_i < p^i$, za $i \in \mathbb{N}$,*

(ii) *$a_i \equiv a_{i+1} \pmod{p^i}$, za $i \in \mathbb{N}$.*

Dokaz. Dokažimo prvo jedinstvenost.
Pretpostavimo da postoji neki drugi niz brojeva iz $\mathbb{N}_0$, $(a'_i)_i \sim (a_i)_i$, koji se razlikuje od niza $(a_i)_i$ za neki indeks i_0, tj. $a_{i_0} \neq a'_{i_0}$ i koji zadovoljava (i) i (ii). Zbog činjenice da je $0 \leq a_{i_0} < p^{i_0}$ i $0 \leq a'_{i_0} < p^{i_0}, a_{i_0}, a'_{i_0} \in \mathbb{N}_0$, vrijedi:

$$a_{i_0} - a'_{i_0} < p^{i_0},$$

iz čega slijedi da $p^{i_0} \nmid (a_{i_0} - a'_{i_0})$, odnosno, $a_{i_0} \not\equiv a'_{i_0} \pmod{p^{i_0}}$.
Za $i \geq i_0$, zbog (ii), sada imamo: $a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \pmod{p^{i_0}}$, odnosno, $a_i \not\equiv a'_i \pmod{p^{i_0}}$. Slijedi da $p^{i_0} \nmid (a_i - a'_i)$, pa je stoga $\mathrm{ord}_p(a_i - a'_i) < i_0$. Sada je $p^{\mathrm{ord}_p(a_i - a'_i)} < p^{i_0}$, a to povlači

$$|a_i - a'_i|_p = \frac{1}{p^{\mathrm{ord}_p(a_i - a'_i)}} > \frac{1}{p^{i_0}}, \tag{3.14}$$

za svaki $i \geq i_0$.
Zaključujemo da (a_i) i (a_i') nisu ekvivalentni u odnosu na p-adsku normu jer ne vrijedi $\lim_{i\to\infty}|a_i - a_i'| = 0$, pa nisu reprezentanti iste klase, a to je kontradikcija s pretpostavkom. Time smo dokazali jedinstvenost.

Dokažimo egzistenciju.
Neka je Cauchyjev niz racionalnih brojeva $(b_i)_i$ proizvoljan reprezentant klase ekvivalencije $[a]$. Želimo naći njemu ekvivalentan niz cijelih brojeva $(a_i)_i$ koji zadovoljava uvjete teorema (i) i (ii).
Obzirom da je $(b_i)_i$ Cauchyjev niz, znamo da, za svaki $j \in \mathbb{N}$, postoji $N(j) \in \mathbb{N}$, takav da za svaki $i, i' \geq N(j)$ vrijedi $|b_i - b_{i'}|_p \leq p^{-j}$, gdje $N(j)$ možemo uzeti kao strogo rastući niz s obzirom na $j \in \mathbb{N}$.
Uočimo da, za svaki $i, i' \geq N(1)$, vrijedi:

$$|b_i|_p = |b_{i'} + b_i - b_{i'}|_p \leq \max\left\{|b_{i'}|_p, |b_i - b_{i'}|_p\right\} \leq \max\left\{|b_{i'}|_p, \frac{1}{p}\right\}.$$

Po definiciji je $|[a]|_p = \lim_{i'\to\infty}\left(|b_{i'}|_p\right)$, odnosno, $|b_{i'}|_p \to |[a]|_p \leq 1$, kad $i' \to \infty$. Također, $\frac{1}{p} \leq 1$, pa slijedi da je, za svaki $i \geq N(1)$, $|b_i|_p \leq 1$. Stoga vrijedi da je $|b_{N_j}|_p \leq 1$, za svaki $j \in \mathbb{N}$.
Sada iz Leme 3.1.24 slijedi da postoji niz cijelih brojeva $(a_j)_{j\in\mathbb{N}}$, $0 \leq a_j < p^j$ i

$$\left|a_j - b_{N(j)}\right|_p \leq \frac{1}{p^j}, \tag{3.15}$$

$j \in \mathbb{N}$. Za takav niz $(a_j)_j$ vrijedi tvrdnja (i).

Pokažimo da za niz $(a_j)_j$ vrijedi tvrdnja (ii), te da je takav niz element klase $[a]$, odnosno $(a_i)_i \sim (b_i)_i$.
Imamo:

$$\begin{aligned}\left|a_{j+1} - a_j\right|_p &= \left|(a_{j+1} - b_{N(j+1)}) + (b_{N(j+1)} - b_{N(j)}) - (a_j - b_{N(j)})\right|_p \\ &\leq \max\left\{\left|a_{j+1} - b_{N(j+1)}\right|_p, \left|b_{N(j+1)} - b_{N(j)}\right|_p, \left|a_j - b_{N(j)}\right|_p\right\} \\ &\leq \max\left\{\frac{1}{p^{j+1}}, \frac{1}{p^j}, \frac{1}{p^j}\right\} = \frac{1}{p^j},\end{aligned}$$

$j \in \mathbb{N}$, pri čemu posljednja nejednakost vrijedi zbog (3.15) i činjenice da je $(b_i)_i$ Cauchyjev niz.
Vrijedi:

$$\left|a_{j+1} - a_j\right|_p = \frac{1}{p^{\mathrm{ord}_p(a_{j+1}-a_j)}} \leq \frac{1}{p^j}, j \in \mathbb{N},$$

pa je

$$\mathrm{ord}_p(a_{j+1} - a_j) \geq j,$$

odnosno, vrijedi

$$p^j \mid (a_{j+1} - a_j),\ j \in \mathbb{N},$$

što je ekvivalentno $a_{j+1} \equiv a_j \pmod{p^j}$, čime je dokazano da vrijedi tvrdnja (ii).

Potrebno je još provjeriti da je niz $(a_i)_i$ doista ekvivalentan nizu $(b_i)_i$. Za proizvoljan $j \in \mathbb{N}$ i za svaki $i \geq N(j)$, vrijedi:

$$\begin{aligned} |a_i - b_i|_p &= \left|(a_i - a_j) + (a_j - b_{N(j)}) - (b_i - b_{N(j)})\right|_p \\ &\leq \max\left\{\left|a_i - a_j\right|_p, \left|a_j - b_{N(j)}\right|_p, \left|b_i - b_{N(j)}\right|_p\right\} \\ &\leq \max\left\{\frac{1}{p^j}, \frac{1}{p^j}, \frac{1}{p^j}\right\} = \frac{1}{p^j}, \end{aligned}$$

pri čemu posljednja nejednakost vrijedi zbog dokazane tvrdnje (ii) (očito je $i \geq j$, a zbog rasta niza $N(j)$ je $N(j) \geq j$) i zbog (3.15). Zaključujemo da (zbog proizvoljnosti $j \in \mathbb{N}$ te zbog zahtjeva $i \geq N(j)$, a $N(j)$ je rastući s obzirom na j) $|a_i - b_i|_p \to 0$, kad $i \to \infty$, pa je $(a_i)_i \sim (b_i)_i$. □

Napomena 3.1.26 ([11])**.** *Primijetimo da, ako p-adski broj* $[a]$ *ne zadovoljava uvjet Teorema 3.1.25, tj. ne vrijedi* $|[a]|_p \leq 1$*, tada p-adski broj* $[a]$ *možemo pomnožiti s* $\frac{1}{|[a]|_p}$*,*[3] *te će za tako dobiveni p-adski broj* $[a'] = \frac{[a]}{|[a]|_p}$ *vrijediti* $|[a']|_p \leq 1$ *i na njega možemo primijeniti prethodni teorem. Time dobivamo da je* $[a']$ *reprezentiran točno jednim nizom* $(a'_i)_i$*, jedinstvenim u* $\mathbb{N}_0$*, koji zadovoljava svojstva (i) i (ii) prethodnog teorema, što znači da je* $[a] = [a']|[a]|_p$ *reprezentiran nizom* $(a_i)_i$*,* $a_i \in \mathbb{N}_0, i \in \mathbb{N}$*, gdje je* $(a_i)_i = (a'_i|[a]|_p)_i$*. Također, pokazali smo i da je to jedinstveni niz nenegativnih cijelih brojeva koji reprezentira* $[a]$*.*

Neka je $[a]$, p-adski broj te $[a']_p = \frac{[a]}{|[a]|_p}$. Sad je $|[a']|_p \leq 1$. Neka je $(a'_j)_j$ jedinstveni reprezentantni niz klase $[a']$ u $\mathbb{N}_0$ iz Teorema 3.1.25. Definirajmo sad algoritamski p-adsku ekspanziju od $[a']$.
Iz uvjeta (i) Teorema 3.1.25 znamo da za svaki član niza $(a'_i)_i$ vrijedi $0 \leq a'_i < p^i, i \in \mathbb{N}$, pa za p^{i-1} postoji jedinstveni $d_{i-1} \in \{0, \ldots, p-1\}$ takav da vrijedi

$$a'_i = d_{i-1}p^{i-1} + r_{i-1},$$

[3] Logaritmiranjem $\log_p$ izraza u Definiciji 3.1.20, možemo definirati $\mathrm{ord}_p[a] := \lim_{n\to\infty} \mathrm{ord}_p(a_n)$, gdje je (a_n) bilo koji reprezentant klase $[a]$. U Definiciji 3.1.20 pokazali smo da limes postoji i da ne ovisi o izboru reprezentanta.

pri čemu je $r_{i-1} \in \{0, \ldots, p^{i-1} - 1\}$. Induktivno, za p^{i-2} postoji jedinstveni $d_{i-2} \in \{0, \ldots, p - 1\}$, takav da vrijedi $r_{i-1} = d_{i-2}p^{i-2} + r_{i-2}, r_{i-2} \in \{0, \ldots, p^{i-2} - 1\}$, pa je

$$a'_i = d_{i-1}p^{i-1} + d_{i-2}p^{i-2} + r_{i-2}.$$

U i-tom koraku d_0 biramo iz skupa $\{0, \ldots, p-1\}$, a $p^{i-i} = 1$, iz čega slijedi $r_0 \leq p^{i-i} - 1 = 0$, pa je $r_0 = 0$ i naš postupak staje.

Članove reprezentantnog niza $(a'_i)_i$ sada možemo zapisati na sljedeći način:

$$a'_i = d_0 + d_1 p + \ldots + d_{i-1}p^{i-1}, \tag{3.16}$$

gdje su $d_i \in \{0, 1, \ldots, p-1\}, i \in \mathbb{N}$. Iz uvjeta (ii) prethodnog teorema znamo da je $a'_i \equiv a'_{i+1} \pmod{p^i}$. Zbog simetričnosti, vrijedi $a'_{i+1} \equiv a'_i \pmod{p^i}$. Sad je, zbog uvjeta $0 \leq a'_{i+1} < p^{i+1}$, a'_{i+1} oblika $a'_{i+1} = a'_i + d_i p^i, d_i \in \{0, \ldots, p-1\}$, odnosno, broju a'_{i+1} smo dodali jedan član, pa je

$$a'_{i+1} = d_0 + d_1 p + \ldots + d_{i-1}p^{i-1} + d_i p^i,$$

gdje su $d_0, d_1, \ldots, d_{i-1}$ isti kao za a'_i.

Dakle, klasu $[a']$ možemo shvatiti kao broj, u oznaci a', zapisan u bazi p koji ima beskonačno mnogo znamenaka s obzirom da svaki put kad prijeđemo s a'_i na a'_{i+1} moramo dodati novi član u zapisu (3.16).

Prema Napomeni 3.1.26, početni p-adski broj $[a]$ reprezentiran je (jedinstvenim) cjelobrojnim nizom u $\mathbb{N}_0$, $(a_i)_i$, gdje je $(a_i)_i = (a'_i p^{-m})_i$, te m kao u [3], stoga članove početnog niza $(a_i)_i$ možemo zapisati kao

$$a_i = \frac{d_0}{p^m} + \frac{d_1}{p^{m-1}} + \ldots + \frac{d_{i-1}}{p^{m-(i-1)}}, i \in \mathbb{N}. \tag{3.17}$$

Našu početnu klasu $[a]$ sada možemo shvatiti kao decimalan broj a zapisan u bazi p koji ima konačno mnogo znamenaka lijevo od decimalne točke (uz negativne potencije broja p), a beskonačno mnogo znamenaka desno od decimalne točke (uz pozitivne potencije broja p). Radi jednostavnosti, koristimo zapis iz Definicije 3.1.27. Preuzeto iz [11].

Definicija 3.1.27 (p-adska ekspanzija p-adskog broja, [11])**.** *Neka je* $[a] \in \mathbb{Q}_p$. *Pišemo*

$$[a] \sim \frac{d_0}{p^m} + \frac{d_1}{p^{m-1}} + \ldots + \frac{d_{m-1}}{p} + d_m + d_{m+1}p + d_{m+2}p^2 + \ldots,$$

pri čemu izraz na desnoj strani relacije $\sim$ *nazivamo* p-adska ekspanzija *broja* $[a] \in \mathbb{Q}_p$.

Primijetimo da, prema gornjem algoritmu, svi p-adski brojevi čija je p-adska norma ≤ 1 imaju p-adsku ekspanziju bez negativnih potencija od p, dok svi p-adski brojevi čija je p-adska norma > 1 imaju p-adsku ekspanziju s konačno mnogo negativnih potencija od p.

U Propoziciji 3.1.29 ćemo dokazati da p-adska ekspanzija broja $[a] \in \mathbb{Q}_p$ doista *konvergira* u $(\mathbb{Q}, |\cdot|_p)$ prema racionalnom broju kojeg ćemo označiti s a i pisati:

$$a := \frac{d_0}{p^m} + \frac{d_1}{p^{m-1}} + \ldots + \frac{d_{m-1}}{p} + d_m + d_{m+1}p + d_{m+2}p^2 + \ldots \tag{3.18}$$

Definicija 3.1.28 (p-adski cijeli broj, [11])**.** *Kažemo da je p-adski broj $[a] \in \mathbb{Q}_p$* p-adski cijeli broj *ako njegova p-adska ekspanzija ne sadrži negativne potencije od p.*
Skup p-adskih cijelih brojeva označavamo s $\mathbb{Z}_p$.

$$\mathbb{Z}_p = \left\{ [a] \in \mathbb{Q}_p : |[a]|_p \leq 1 \right\}.$$

Primijetimo da iz Napomene 3.1.26 slijedi da p-adska ekspanzija broja $[a] \in \mathbb{Q}_p$ ne sadrži negativne potencije od p ako i samo ako je $|[a]|_p \leq 1$.

Propozicija 3.1.29 ([11])**.** *Neka je $(d_i)_{i=-m}^{\infty}$ niz p-adskih cijelih brojeva. Tada je red*

$$\sum_{i=-m}^{\infty} d_i p^i,$$

konvergentan u normiranom prostoru $\mathbb{Q}_p$.

Dokaz. Označimo N-tu parcijalnu sumu reda $\sum_{i=-m}^{\infty} d_i p^i$ s S_N, $N \in \mathbb{N}$. Tada je

$$S_N = \frac{d_{-m}}{p^m} + \frac{d_{-m+1}}{p^{m-1}} + \ldots + d_0 + d_1 p + \ldots + d_N p^N.$$

Dokažimo da niz parcijalnih suma konvergira u $\mathbb{Q}_p$.
Uzmimo proizvoljni $\varepsilon > 0$ te $N \in \mathbb{N}$ dovoljno velik tako da $\frac{1}{p^N} < \varepsilon$. Sada za svaki $M \in \mathbb{N}$, $M > N$, vrijedi:

$$\begin{aligned} |S_M - S_N|_p &= |d_M p^M + d_{M-1} p^{M-1} + \ldots + d_{N+1} p^{N+1}|_p \\ &\leq \max\{|d_M p^M|_p, \ldots, |d_{N+1} p^{N+1}|_p\} \\ &< \frac{1}{p^N}, \end{aligned}$$

pa zaključujemo da je niz parcijalnih suma Cauchyjev, dakle, u p-adskoj normi konvergira u $\mathbb{Q}_p$, a tada i red $\sum_{i=-m}^{\infty} d_i p^i$ konvergira u $\mathbb{Q}_p$. Zbog potpunisti $\mathbb{Q}_p$ suma reda je također p-adski broj. □

Specijalno, ako stavimo $d_i \in \{0, ..., p-1\}$ (trivijalno p-adski brojevi), po Propoziciji 3.1.29 znamo da desna strana jednakosti (3.18) konvergira u $(\mathbb{Q}, |\cdot|_p)$ i time je jednakost opravdana. Štoviše, limes je klasa konstantnog niza $[(a, a, \ldots)]$, gdje je $a \in \mathbb{Q}$, pa limes u tom slučaju možemo poistovjetiti i s racionalnim brojem $a \in \mathbb{Q}$. Na taj način p-adskom broju u smislu niza pridružujemo racionalni broj koji također zovemo p-adskim brojem. Stoga možemo u Definiciji 3.1.28 pisati i $\mathbb{Z}_p = \{a \in \mathbb{Q} : |[(a, a, \ldots)]|_p \leq 1\}$, a onda slijedi i

$$\mathbb{Z}_p = \{a \in \mathbb{Q} : |a|_p \leq 1\}.$$

Primijetimo da postupak možemo provesti i obrnuto, tj. ako je dan racionalni broj s nekom p-adskom ekspanzijom, možemo jednoznačno naći klasu koja odgovara toj ekspanziji. Uzmimo p-adsku ekspanziju $a = \frac{d_0}{p^m} + \frac{d_1}{p^{m-1}} + \ldots + \frac{d_{m-1}}{p} + d_m + d_{m+1}p + d_{m+2}p^2 + \ldots$. Tada niz parcijalnih suma p-adske ekspanzije $(S_N)_N$ predstavlja jedinstveni konvergentan niz u $\mathbb{Q}$, a time i Cauchyjev niz u $(\mathbb{Q}, |\cdot|_p)$. Njegova klasa ekvivalencije predstavlja element iz $\mathbb{Q}_p$. Jedan od reprezentanata te klase je i $(a, a, a, \ldots)$. Preuzeto iz [11].

Naposlijetku, primijetimo da nam Teorem 3.1.25 garantira jedinstvenost p-adske ekspanzije.

3.1.3 Aritmetika u $\mathbb{Q}_p$

Opišimo algoritme zbrajanja i množenja p-adskih brojeva. p-adska ekspanzija omogućava nam izvođenje računskih operacija način vrlo sličan onome na koji smo navikli, primjerice, zbrajajući prirodne ili cijele brojeve.

Neka su a i b cijeli p-adski brojevi s ekspanzijama $a = a_0 + a_1 p + a_2 p^2 + \ldots$ i $b = b_0 + b_1 p + b_2 p^2 + \ldots$. Zbrajanje provodimo po komponentama. Prva komponenta zbroja brojeva a i b bit će $a_0 + b_0$ ako je $a_0 + b_0 \leq p - 1$. U suprotnom, prva je komponenta $a_0 + b_0 - p$ pri čemu "prenosimo jedinicu" sljedećoj komponenti. Na taj način osiguravamo da se sve p-adske znamenke dobivenog niza nalaze u skupu $\{0, 1, \ldots, p-1\}$.
Slično, umnožak dva p-adska broja dobit ćemo množenjem odgovarajućih komponenata njihove p-adske ekspanzije i "prenošenjem jedinice" kako bismo dobili samo znamenke unutar skupa $\{0, 1, \ldots, p-1\}$. Tako definirano množenje nije ništa drugo nego li uobičajeno množenje na koje smo navikli. Jedina je razlika što postupak provodimo s lijeva na desno i, zbog beskonačnog zapisa p-adskih brojeva, postupak nikad ne staje.

Provjerimo još da zbroj p-adskih ekspanzija p-adskih brojeva a i b općenito odgovara zbroju njima odgovarajućih klasa $[a]$ i $[b]$. Neka su $(a_n)_{n\in\mathbb{N}}$ i $(b_n)_{n\in\mathbb{N}}$ reprezentantni nizovi za klase $[a]$ i $[b]$ respektivno. Tada je njihov zbroj klasa $[a_n + b_n]$. Prema (3.17) svaki član niza (a_n) možemo zapisati kao

$$a_n = \frac{d_0}{p^m} + \frac{d_1}{p^{m-1}} + \ldots + \frac{d_{n-1}}{p^{m-(n-1)}},$$

za svaki $n \in \mathbb{N}$, gdje su $d_n \in \{0, \ldots, p-1\}$.
Analogno, svaki član niza (b_n) možemo zapisati kao

$$b_n = \frac{v_0}{p^m} + \frac{v_1}{p^{m-1}} + \ldots + \frac{v_{n-1}}{p^{m-(n-1)}},$$

za svaki $n \in \mathbb{N}$, gdje su $v_n \in \{0, \ldots, p-1\}$. Primijenimo li sada opisani algoritam za zbrajanje imamo: $a_0 + b_0 = \frac{d_0+v_0}{p^m}$, ako je $d_0 + v_0 \leq p-1$, odnosno, ako je $d_0 + v_0 \geq p$, $a_0 + b_0 = \frac{d_0+v_0-p}{p^m}$, gdje je $d_0 + v_0 - p \leq p-1$, iz čega vidimo da se jedinica „prenosi" na sljedeću potenciju od p u razvoju. Tako nastavljamo dalje za $a_n + b_n$, $n \in \mathbb{N}$. Preuzeto iz [11].

Analogno bismo pokazali da je gore opisano množenje ekspanzija p-adskih brojeva a i b ekvivalentno množenju klasa $[a]$ i $[b]$.

3.2 Prsten $\mathbb{Z}_p$

U ovom ćemo potpoglavlju pokazati da je $\mathbb{Z}_p$ s operacijama zbrajanja i množenja komutativni prsten. Očito je da će zbroj i umnožak dva elementa skupa $\mathbb{Z}_p$ također biti element skupa $\mathbb{Z}_p$ zbog pozitivnosti svih potencija od p u p-adskoj ekspanziji.

Propozicija 3.2.1 (Prsten $\mathbb{Z}_p$, [13])**.** *Skup cijelih p-adskih brojeva, $\mathbb{Z}_p$, je komutativni prsten.*

Dokaz. Provjerimo da $\mathbb{Z}_p$ ima strukturu prstena.

- Komutativnost zbrajanja se nasljeđuje iz komutativnosti zbrajanja u polju $\mathbb{Q}_p$.
- Asocijativnost zbrajanja se nasljeđuje iz asocijativnosti zbrajanja u polju $\mathbb{Q}_p$.
- Neutralni element za zbrajanje: U skupu p-adskih brojeva postoji neutralni element za zbrajanje

$$0_p = \sum_{k\geq 0} 0p^k.$$

- Suprotni element za zbrajanje: Neka je $n_p \in \mathbb{Z}_p$ definiran s

$$n_p = \sum_{k\geq 0} n_k p^k,$$

a $n_p^* \in \mathbb{Z}_p$ neka je

$$n_p^* = \sum_{k\geq 0} (p-1-n_k)p^k.$$

Lako se provjeri da je $n_p + n_p^* = -1_p$, iz čega slijedi da je $n_p + (n_p^* + 1_p) = 0_p$. Da bismo zaključili da je $n_p^* + 1_p$ suprotni element od n_p, provjerimo još da je $-1_p \in \mathbb{Z}_p$. 1_p u p-adskoj ekspanziji zapisujemo kao $1_p = 1 + 0p + 0p^2 + \ldots$. Neka $b \in \mathbb{Z}_p$ ima p-adsku ekspanziju $b = (p-1) + (p-1)p + (p-1)p^2 + \ldots$. Zbrojimo sada 1_p i b po komponentama.
Za prvu komponentu imamo $1 + (p-1) = p$, pa je prva komponenta 0, pri čemu jedinicu prenosimo sljedećoj komponenti. Vidimo da je tada i druga komponenta nula. Preostale komponente su također 0, pa je $1_p + b = 0_p$, odnosno, $b = -1_p \in \mathbb{Z}_p$.

Dakle, za svaki $n_p \in \mathbb{Z}_p$

$$n_p = \sum_{k\geq 0} n_k p^k,$$

suprotni element je

$$-n_p = \sum_{k\geq 0} (p-1-n_k)p^k + 1_p.$$

- Komutativnost množenja se nasljeđuje iz komutativnosti množenja u polju $\mathbb{Q}_p$.
- Asocijativnost množenja se nasljeđuje iz asocijativnosti množenja u polju $\mathbb{Q}_p$.
- Svojstvo distributivnosti se nasljeđuje iz distributivnosti u polju $\mathbb{Q}_p$

Zaključujemo da je $\mathbb{Z}_p$ komutativni prsten. □

Primijetimo da za p-adski broj a, pri čemu je $a = \sum_{i\geq 0} p^i$, vrijedi

$$a = \sum_{i\geq 0} p^i = \frac{1}{1-p},$$

pa $1 - p$ ima inverzni element za množenje u $\mathbb{Z}_p$.

Znamo da je $1_p = [(1, 1, \ldots)]$ neutralni element za množenje u polju $\mathbb{Q}_p$. Naime, 1_p ima p-adsku ekspanziju $1 + 0p + 0p^2 + \ldots \in \mathbb{Z}_p$, pa je to neutralni element za množenje u $\mathbb{Z}_p$.

Općenito, vrijedi

$$p \cdot \sum_{i \geq 0} a_i p^i = a_0 p + a_1 p^2 + \ldots \neq 1 + 0p + 0p^2 + \ldots,$$

pa slijedi da p nema multiplikativni inverz u $\mathbb{Z}_p$. Sličnim argumentom pokazuje se da p-adski brojevi čija je prva znamenka $a_0 = 0$ nemaju multiplikativni inverz u $\mathbb{Z}_p$. Preuzeto iz [11].

3.3 Homeomorfizam $\mathbb{Z}_2$ i Cantorovog skupa

Prisjetimo se nekih metričkih pojmova. Neka je (X, d) metrički prostor i neka je $x \in X$. *Otvorena kugla* ([17]) polumjera r sa središtem u x je skup točaka u X čija je udaljenost od x manja od r, odnosno

$$B(x, r) = \{y \in X : d(x, y) < r\}.$$

Za skup U kažemo da je *otvoren* u X ako za svaki $x \in U$ postoji otvorena kugla sadržana u U takva da sadrži x, tj. za svaki $x \in U$ postoji $r > 0$ i $a \in U$ takvi da je $x \in B(a, r) \subseteq U$. Kažemo da je skup *zatvoren* ako mu je komplement otvoren.

Teorem 3.3.1 ([17])**.** *Sfera*

$$S(x, r) = \{y \in \mathbb{Q} : |x - y|_p = r\}$$

je otvoren skup u $\mathbb{Q}_p$.

Dokaz. Neka je $y \in S(x, r)$ proizvoljan. Pokazat ćemo da je $B\left(y, \frac{r}{2}\right) \subseteq S(x, r)$. Neka je $z \in B\left(y, \frac{r}{2}\right)$ proizvoljan. Pokažimo da je $z \in S(x, r)$. Vrijedi $|z - y|_p < |y - x|_p = r$. Također, vrijedi $|z - x|_p = |z - y + y - x|_p \leq \max\{|z - y|_p, |y - x|_p\}$. Kako je norma $|\cdot|_p$ nearhimedska, tj. za $|a|_p \neq |b|_p$ vrijedi $|a + b|_p = \max\{|a|_p, |b|_p\}$, a u našem je slučaju $|z - y|_p < |y - x|_p$, slijedi $|z - x|_p = |y - x|_p = r$. Dakle, $|z - x|_p = r$, tj. $z \in S(x, r)$, iz čega zaključujemo da je $B\left(y, \frac{r}{2}\right) \subseteq S(x, r)$, te je tvrdnja dokazana. □

Korolar 3.3.2 ([17])**.** *Svaka otvorena kugla u* $\mathbb{Q}_p$ *je i otvoren i zatvoren skup.*

Dokaz. Neka je $B(a, r)$ otvorena kugla sa središtem u a polumjera r. S obzirom na to da je otvorena kugla trivijalno otvorena po definiciji jer oko svake točke sadrži samu sebe,

jasno je da sadrži otvorenu kuglu oko svake svoje točke. Pokažimo da je otvorena kugla i zatvoreni skup. Promotrimo komplement skupa $B(a,r)$. Komplement možemo zapisati kao

$$\mathbb{Q}_p \setminus B(a,r) = \{y \in \mathbb{Q}_p : |x-y|_p \geq r\} = A \cup B,$$

gdje je $A = \{y \in \mathbb{Q}_p : |x-y|_p > r\}$ i $B = \{y \in \mathbb{Q}_p : |x-y|_p = r\} = S(a,r)$. Dokažimo da je komplement otvorene kugle otvoreni skup. Prema Teoremu 3.3.1, B je otvoren skup. Da bismo pokazali da je i A otvoreni skup, izabrat ćemo $y \in A$, proizvoljan. Tada je $|y-a|_p = r^* > r$. Dokazat ćemo da je $B(y, r^* - r) \subseteq A$. Pretpostavimo suprotno, tj. postoji $z \in B(y, r^* - r)$ takav da je $|z-a|_p \leq r$. Tada imamo

$$r^* = |y-a|_p \leq |y-z|_p + |z-a|_p \leq \max\{|y-z|_p, |z-a|_p\} \leq \max\{r^* - r, r\} < r^*,$$

što je kontradikcija, pa mora biti $B(y, r^* - r) \subseteq A$. Time je dokazano da je A otvoren skup, a kako je $\mathbb{Q}_p \setminus B(a,r)$ unija dva otvorena skupa zaključujemo da je otvoren, pa je njegov komplement, $B(a,r)$, zatvoren skup. □

U posljednjem teoremu ovoga poglavlja dokazat ćemo postojanje *homeomorfizma* između skupa $\mathbb{Z}_2$ i Cantorovog skupa. Prije samog teorema, prisjetimo se definicije homeomorfizma.

Definicija 3.3.3 ([8]). *Neka su (X,τ) i (Y,ν) topološki prostori, a $f : X \to Y$ preslikavanje sa svojstvima*

(i) *f je bijekcija,*

(ii) *$f(U) \in \tau$, za svaki $U \in \tau$,*

(iii) *$f^{-1}(V) \in \tau$, za svaki $V \in \nu$.*

Tada kažemo da je f homeomorfizam *prostora X i Y.*

Kažemo da je topološki prostor (X,τ) *homeomorfan* s (Y,ν) i pišemo $X \cong Y$, ako postoji homeomorfizam $f : X \to Y$.

Teorem 3.3.4 ([17]). *Neka je $p = 2$. Prostor 2-adskih (ili diadskih) brojeva $\mathbb{Z}_2$ s 2-adskom normom homeomorfan je Cantorovom skupu C, u naslijeđenoj euklidskoj topologiji.*

Dokaz. Da bismo dokazali tvrdnju teorema, naći ćemo preslikavanje između skupa $\mathbb{Z}_2$ i skupa C te pokazati da je takvo preslikavanje homeomorfizam. Neka je $a \in \mathbb{Z}_2$, s 2-adskom ekspanzijom

$$\sum_{k=0}^{\infty} a_k 2^k, \tag{3.19}$$

gdje je $a_k \in \{0, 1\}$. S druge strane, iz Poglavlja 1 znamo da svaki element Cantorovog skupa možemo zapisati kao

$$\sum_{k=1}^{\infty} \frac{b_k}{3^k}, \tag{3.20}$$

gdje je $b_k \in \{0, 2\}$. Neka je F funkcija definirana s

$$F : \sum_{k=0}^{\infty} a_k 2^k \to \sum_{k=0}^{\infty} \frac{2a_k}{3^{k+1}}.$$

S obzirom na to da i p-adski brojevi i elementi Cantorovog skupa imaju jedinstveni prikaz u oblicima (3.19) i (3.20), slijedi da je funkcija F injekcija, odnosno, ako je $F(a) = F(b)$, onda je $a = b$. Uz to, $\sum_{k=0}^{\infty} \frac{2a_k}{3^{k+1}}$, $a_k \in \{0, 1\}$, predstavlja sve elemente Cantorovog skupa, pa je funkcija F surjekcija, te zaključujemo da je bijekcija.

Preostaje pokazati da su F i F^{-1} neprekidne u danom paru topologija. Pokažimo neprekidnost funkcije F u točki $\sum_{k=0}^{\infty} a_k 2^k$.

Uzmimo $\varepsilon > 0$. Tražimo $\delta > 0$ takav da za svaki $\sum_{k=0}^{\infty} a'_k 2^k$ takav da $|\sum_{k=0}^{\infty}(a_k - a'_k)2^k|_p < \delta$ vrijedi

$$\left| 2 \sum_{k=0}^{\infty} \frac{a_k - a'_k}{3^{k+1}} \right| < \varepsilon,$$

pri čemu $|\cdot|$ označava apsolutnu vrijednost (udaljenost slika u euklidskoj topologiji). Za dani $\varepsilon > 0$ pronađimo $N \in \mathbb{N}$ takav da je $\frac{1}{3^N} < \varepsilon$. Primijetimo da je razlika

$$\left| \sum_{k=0}^{\infty} \frac{2a_k}{3^{k+1}} - \sum_{k=0}^{\infty} \frac{2a'_k}{3^{k+1}} \right| < \frac{1}{3^N}$$

ako i samo ako je $a_k = a'_k$, $k = 0, \ldots, N + 1$, tj. ako se a_k i a'_k podudaraju u prvih $N + 1$ 'znamenaka'. Isto tako,

$$\left| \sum_{k=0}^{\infty} a_k 2^k - \sum_{k=0}^{\infty} a'_k 2^k \right|_p < \frac{1}{2^M}$$

ako i samo ako je $a_k = a'_k$ za $k = 0, \ldots, M$. Za dani $\varepsilon > 0$, stavimo $M := N + 1$ i $\delta = 2^{-M}$. Sada, s obzirom na to da i $\frac{1}{3^N}$ i $\frac{1}{2^{N+1}}$ konvergiraju u nulu kad $N \to \infty$, zaključujemo da je F neprekidna funkcija.

Slično se pokazuje i neprekidnost inverzne funkcije, F^{-1}. □

Bibliografija

[1] *Mali Fermatov i Eulerov teorem*, 2016, https://mnm.hr/wp-content/uploads/2015/10/mali_fermat_i_euler.pdf.

[2] *Fermat's Little Theorem / Corollary 4*, https://proofwiki.org/wiki/Fermat%27s_Little_Theorem/Corollary_4.

[3] R. J. Plymen A. J. Baker, *p-adic methods and their applications*, Oxford University Press, Oxford, 1992.

[4] D. M. Bressoud, *A radical approach to Lebesgue's theory of integration*, Cambridge University Press, Cambridge, 2008.

[5] D. C. Collins, *Continued fractions*, The MIT Undergraduate Journal of Mathematics **1** (1999), 11–20.

[6] T. W. Cusick, *Sums of sets of continued fractions*, Proceedings of the American Mathematical Society **27** (1971), br. 1, 35–38.

[7] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[8] B. Guljaš, *Metrički prostori*, nastavni materijal, 2010, https://web.math.pmf.unizg.hr/~guljas/skripte/metprost.pdf.

[9] T. Kemp, *Cauchy's Construction of R*, Dostupno na: www.math.ucsd.edu/˜tkemp A **140** (2016).

[10] A. Y. Khinchin, *Continued fractions*, Dover Publications Inc., New York, 1997.

[11] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, sv. 58, Springer Science & Business Media, New York, 2012.

[12] K. O. May, *Mathematics: Continued Fractions. A. Ya. Khinchin, Translated from the third Russian edition (Moscow, 1961) by Scripta Technica*, Science **145** (1964), br. 3631, 478–478.

[13] A. M. Robert, *A course in p-adic analysis*, sv. 198, Springer Science & Business Media, New York, 2013.

[14] N. A. Scoville, *The Cantor Set Before Cantor: A Mini-Primary Source Project for Analysis and Topology Students*, Convergence, The Mathematical Association of America (2019).

[15] T. Sundstrom, *9.3: Uncountable Sets*, 2022, https://math.libretexts.org/Bookshelves/Mathematical_Logic_and_Proof/Book%3A_Mathematical_Reasoning__Writing_and_Proof_(Sundstrom)/09%3A_Finite_and_Infinite_Sets/9.03%3A_Uncountable_Sets.

[16] J. A. Thorne, *p-adic analysis, p-adic arithmetic*, Harvard Mathematics Department Summer Tutorials, 2010.

[17] R. W. Vallin, *The elements of Cantor sets: with applications*, John Wiley & Sons, New Jersey, 2013.

Sažetak

Ovaj diplomski rad bavi se raznim analitičkim konstrukcijama Cantorovog skupa. U prvom poglavlju upoznajemo se s Cantorovim skupom i konstruiramo ga na tzv. geometrijski način te objašnjavamo neka njegova svojstva (duljinu, kardinalitet i gustoću u skupu $\mathbb{R}$).

U drugom poglavlju bavimo se prvom konstrukcijom Cantorovog skupa preko tzv. *verižnih razlomaka*. Definiramo verižne razlomke, dokazujemo postojanje konačnog prikaza svakog racionalnog broja u obliku verižnog razlomka i postojanje razvoja u verižni razlomak za svaki realni broj, odnosno, dokazujemo konvergenciju beskonačnih verižnih razlomaka. Naposlijetku dokazujemo da je, za cijeli broj k, $k \geq 2$, skup svih realnih brojeva α, takvih da je $0 \leq \alpha \leq k^{-1}$ i takvih da razvoj broja α u verižni razlomak ne sadrži parcijalni kvocijent manji od k, Cantorov skup.

U trećem poglavlju konstruiramo Cantorov skup kao homeomorfnu sliku prstena cijelih p-adskih brojeva $\mathbb{Z}_p$, p prost broj. Prvo definiramo p-adske brojeve i cijele p-adske brojeve. Definiramo p-adsku normu i p-adsku udaljenost na polju $\mathbb{Q}$ te dokazujemo da polje $\mathbb{Q}$ s p-adskom normom nije potpuno. Upotpunjujemo polje $\mathbb{Q}$ poljem klasa ekvivalencije Cauchyjevih nizova, $\mathbb{Q}_p$. Nakon toga, pokazujemo ekvivalenciju polja $\mathbb{Q}_p$ kao skupa klasa ekvivalencija nizova i beskonačnih p-adskih ekspanzija koje konvergiraju u p-adskoj normi na $\mathbb{Q}$. Konačno, pokazujemo postojanje homeomorfizma između prstena cijelih p-adskih brojeva $\mathbb{Z}_p$ i Cantorovog skupa u naslijeđenoj euklidskoj topologiji.

Summary

This thesis focuses on different geometric and analytical constructions of the Cantor set. The first chapter is an introduction to Cantor sets and explains a geometric construction. We also prove the basic properties of Cantor sets (length, cardinality and density in $\mathbb{R}$).

The second chapter deals with a construction of a Cantor set using continued fractions. We define continued fractions, prove the existence of a finite representation of every rational number in the form of a continued fraction and the existence of an expansion into a continued fraction for every real number. That is, we prove the convergence of infinite continued fractions. Finally, we prove that, for an integer k, $k \geq 2$, the set of all real numbers α such that $0 \leq \alpha \leq k^{-1}$ and such that the expansion of number α into a continued fraction does not contain a partial quotient smaller than k is a Cantor set.

In the third chapter we construct a Cantor set as a homeomorphic image of the ring of p-adic integers $\mathbb{Z}_p$, where p is a prime number. First, we define p-adic numbers and p-adic integers. We define p-adic norm and p-adic distance on the field $\mathbb{Q}$ and prove that the field $\mathbb{Q}$ with p-adic norm is not complete. We complete the field $\mathbb{Q}$ as a field of equivalence classes of Cauchy sequences, $\mathbb{Q}_p$, with an appropriate norm. After that, we show the equivalence of the field $\mathbb{Q}_p$ regarded as the set of equivalence classes of sequences and of p-adic expansions that converge in the p-adic norm on $\mathbb{Q}$. Finally, we show the existence of a homeomorphism between the space of p-adic integers $\mathbb{Z}_p$ as a subspace of $\mathbb{Q}_p$ and a Cantor set with Euclidean topology.

Životopis

Rođena sam 2. lipnja 1995. godine u Rijeci. Završila sam osnovnu školu Vladimira Nazora u Pazinu, a nakon toga, također u Pazinu, Gimnaziju i strukovnu školu Jurja Dobrile (smjer opća gimnazija). Tijekom srednjoškolskog obazovanja završila sam 1. stupanj Govorničke škole „Ivo Škarić“ te sam sudjelovala na školskim i županijskim natjecanjima iz logike, filozofije, hrvatskog jezika i atletike. Neposredno nakon završetka gimnazije upisala sam Prirodoslovno-matematički fakultet u Zagrebu, Matematički odsjek. Akademske godine 2016./17. držala sam demonstrature iz kolegija Analitička geometrija. Godine 2019. upisala sam diplomski studij Matematika - smjer nastavnički, koji trenutno pohađam.