Incidencijske algebre

Bujan, Marija

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Marija Bujan

Incidencijske algebre

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Vedran Krčadinac

Zagreb, ožujak 2023.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____ .

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

1 Uvod

U ovom radu obrađeni su elementi teorije incidencijskih algebri i njezine primjene u kombinatorici. Rad je podjeljen u tri poglavlja.

U prvom poglavlju definirali smo parcijalno uređen skup, lokalnu konačnost parcijalno uređenog skupa te naveli nekoliko primjera. Nakon definicije komutativnog prstena s jedinicom uvodimo pojam incidencijske algebre. Incidencijska algebra lokalno konačnog parcijalno uređenog skupa X nad komutativnim prstenom s jedinicom R, u oznaci $I(X, R)$, je skup svih funkcija $f\colon X \times X \to R$ takvih da je $f(x, y) = 0$ ako $x \not\leq y$. Definirali smo operacije u incidencijskoj algebri te uveli neke važne funkcije poput Kroneckerove i zeta funkcije. U prvom teoremu pokazali smo da je $I(X, R)$ asocijativna R-algebra s jedinicom, a u sljedećem teoremu dana je karakterizacija invertibilnih funkcija u $I(X, R)$. Pred kraj prvog poglavlja pokazali smo da se incidencijska algebra $I(X, R)$ može uložiti u algebru trokutastih matrica.

Incidencijske algebre razvile su se kao prirodno okruženje za generalizaciju formule Möbiusove inverzije u teoriji brojeva. U drugom poglavlju definirali smo klasičnu Möbiusovu funkciju te iskazali teorem klasične Möbiusove inverzije. Središnji dio drugog poglavlja je teorem o generaliziranim formulama Möbiusove inverzije. Za računanje Möbiusove funkcije μ iskoristili smo činjenicu da je Möbiusova funkcija inverzna zeta funkciji. Također korisna nam je bila i činjenica da se za izračun vrijednosti $\mu(x, y)$ dovoljno ograničiti na konačan parcijalno uređen skup $[x, y]$. Korištenjem prethodnih tvrdnji izračunali smo Möbiusovu funkciju nekih parcijalno uređenih skupova koji se mogu zapisati kao direktni produkt jednostavnijih parcijalno uređenih skupova. Također, istražili smo i dio veze između Möbiusove inverzije i algebarske topologije te na primjerima iz kombinatorike pokazali primjenu Möbiusove inverzije.

U trećem poglavlju uvodimo pojam podalgebre. Ako na skupu neprazних intervala od X imamo definiranu relaciju ekvivalencije, onda funkciju f iz incidencijske algebre $I(X, R)$ za koju vrijedi $[x, y]E[u, v]$ povlači $f(x, y) = f(u, v)$ nazivamo E-funkcijom. Skup svih E-funkcija označili smo s $I(X_E, R)$ te smo uz dodatne definicije pojmova vezanih za relaciju E pokazali vezu između $I(X, R)$ i $I(X_E, R)$. Prethodno pokazana veza ilustrirana je primjerom gdje je X konačan parcijalno uređen skup, a R polje. Nadalje, definirali smo pojam reducirane incidencijske algebre i standardne reducirane incidencijske algebre te dali karakterizaciju reducirane incidencijske podalgebre konačnog parcijalno uređenog skupa nad poljem. Na samom kraju trećeg poglavlja dana su dva primjera koja nam pokazuju vezu reduciranih incidencijskih podalgebri s prstenima formalnih redova potencija.

2 Incidencijske algebre

Definicija 2.1. *Neka je X neprazan skup. Svaki podskup $\leq$ od $X \times X$ nazivamo* ***binarnom relacijom****. Činjenicu $(x, y) \in \leq$ zapisujemo i $x \leq y$. Kažemo da je binarna relacija $\leq$:*

i) ***refleksivna****, ako za svaki $x \in X$ vrijedi $x \leq x$,*

ii) ***irefleksivna****, ako ne postoji $x \in X$ takav da vrijedi $x \leq x$,*

iii) ***simetrična****, ako za sve $x, y \in X$ koji imaju svojstvo $x \leq y$ vrijedi $y \leq x$,*

iv) ***antisimetrična****, ako za sve $x, y \in X$ koji imaju svojstvo $x \leq y$ i $y \leq x$ vrijedi $x = y$,*

v) ***tranzitivna****, ako za sve $x, y, z \in X$ koji imaju svojstvo $x \leq y$ i $y \leq z$ vrijedi $x \leq z$,*

vi) ***relacija ekvivalencije****, ako je refleksivna, simetrična i tranzitivna,*

vii) ***relacija parcijalnog uređaja****, ako je refleksivna, antisimetrična i tranzitivna.*

Skup X s relacijom parcijalnog uređaja $\leq$ nazivamo ***parcijalno uređenim skupom****. Označavamo ga s $(X, \leq)$.*

Definicija 2.2. *Neka je $(X, \leq)$ parcijalno uređen skup te $x, z \in X$.* ***Interval*** *ili* ***segment*** *od x do z je skup $[x, z] = \{y \in X \mid x \leq y \leq z\}$. Parcijalno uređen skup je* ***lokalno konačan*** *ako je svaki segment od X konačan.*

Definicija 2.3. ***Lanac*** *u parcijalno uređenom skupu $(X, \leq)$ je podskup $L \subseteq X$ takav da za sve $x, y \in L$ vrijedi $x \leq y$ ili $y \leq x$.* ***Antilanac*** *u parcijalno uređenom skupu $(X, \leq)$ je podskup $A \subseteq X$ takav da za sve $x, y \in A, x \neq y$ vrijedi $x \not\leq y$ i $y \not\leq x$.*

Navedimo nekoliko primjera.

Primjer 2.4. *1) $(\mathbb{R}, \leq)$ je parcijalno uređen skup gdje je $\leq$ prirodni uređaj na $\mathbb{R}$. Štoviše, on je totalno uređen, to jest svaka dva njegova elementa su usporediva. Bilo koji podskup skupa $\mathbb{R}$ čini lanac.*

2) $(\mathcal{P}(\{1, 2, 3\}), \subseteq)$ je parcijalno uređen skup. Uređaj $\subseteq$ je pravi parcijalni uređaj jer postoje elementi skupa $\mathcal{P}(\{1, 2, 3\})$ koji nisu usporedivi. Primjer antilanca u danom parcijalno uređenom skupu je $A = \{\{1\}, \{2\}, \{3\}\}$.

3) $(\mathbb{N}, |)$ *pri čemu je* $|$ *relacija djeljivosti je pravi parcijalno uređen skup. On je lokalno konačan jer za* $x, y \in \mathbb{N}$ *segment* $[x, y]$ *sadrži samo djelitelje broja* y *kojih ima konačno mnogo.*

4) $(\mathcal{P}(S), \subseteq)$ *je pravi parcijalno uređen skup pri čemu je* S *bilo koji skup koji ima bar dva elementa. On je lokalno konačan ako je skup* S *konačan.*

Definicija 2.5. *Trojku* $(R, +, \cdot)$ *koja se sastoji od nepraznog skupa* R *i dvije binarne operacije zovemo* ***prstenom*** *ukoliko je za operacije zbrajanja* $+\colon R \times R \to R$ *i množenja* $\cdot\colon R \times R \to R$ *ispunjeno sljedeće:*

i) $(R, +)$ *je komutativna grupa, to jest vrijedi:*

- $(x + y) + z = x + (y + z), \quad \forall x, y, z \in R$ *(asocijativnost)*
- $x + y = y + x, \quad \forall x, y \in R$ *(komutativnost)*
- $\exists\, 0 \in R\colon \quad x + 0 = 0 + x = x, \quad \forall x \in R$ *(neutralni element)*
- $\forall x \in R,\ \exists - x \in R\colon \quad x + (-x) = -x + x = 0$ *(suprotni element)*

ii) $(R, \cdot)$ *je polugrupa, to jest vrijedi:*

- $(x \cdot y) \cdot z = x \cdot (y \cdot z), \quad \forall x, y, z \in R$ *(asocijativnost)*

iii) vrijedi distributivnost množenja prema zbrajanju, to jest vrijedi:

- $x \cdot (y + z) = x \cdot y + x \cdot z, \quad \forall x, y, z \in R$
- $(x + y) \cdot z = x \cdot z + y \cdot z, \quad \forall x, y, z \in R.$

Ako postoji ***jedinični element****, ili kraće* ***jedinica****,* 1 *takva da je* $1 \cdot x = x \cdot 1 = x$ *za sve* $x \in R$*, onda kažemo da je* R ***prsten s jedinicom****. Prsten* R *je* ***komutativan prsten*** *ako je* $x \cdot y = y \cdot x$ *za sve* $x, y \in R$*.*

Neka je $(R, +, \cdot)$ prsten s jedinicom. Kažemo da je $x \in R$ *invertibilni element* ako postoji $x^{-1} \in R$ takav da $x \cdot x^{-1} = x^{-1} \cdot x = 1$. Pretpostavimo da postoji $m \in \mathbb{N}$ takav da vrijedi $mx = 0$, za sve $x \in R$. *Karakteristika prstena* R je minimalan takav m koji zadovoljava prethodnu jednakost. Ukoliko takav m ne postoji, kažemo da je prsten R *karakteristike nula.*

Lema 2.6. *Neka je* R *prsten s jedinicom i* $s \in R$*. Ako* s *ima i desni i lijevi inverz, onda je* s *invertibilni element.*

Dokaz. Neka su $r, t \in R$ takvi da je $rs = st = 1$. Tada je $t = (rs)t = r(st) = r$. □

Ukoliko postoji, element x^{-1} je jedinstven i zovemo ga *(multiplikativnim) inverzom* od x.

Definicija 2.7. *Neka je $(X, \leq)$ lokalno konačan parcijalno uređen skup i R komutativni prsten s jedinicom.* ***Incidencijska algebra*** *$I(X, R)$ je skup svih funkcija $f\colon X \times X \to R$ takvih da je $f(x, y) = 0$ ako ne vrijedi $x \leq y$, to jest $I(X, R) = \{f\colon X \times X \to R \mid f(x, y) = 0 \text{ ako } x \not\leq y\}$. Operacije na $I(X, R)$ definiramo s:*

$$\begin{aligned} (f + g)(x, y) &= f(x, y) + g(x, y) && \text{(zbrajanje)} \\ (r \cdot f)(x, y) &= r \cdot f(x, y) && \text{(množenje skalarom)} \\ (f * g)(x, y) &= \sum_{x \leq z \leq y} f(x, z) g(z, y) && \text{(produkt ili konvolucija)} \end{aligned}$$

gdje su $f, g \in I(X, R),\ r \in R,\ x, y, z \in X$.

Operacije na $I(X, R)$ su dobro definirane, to jest za $f, g \in I(X, R)$ te $r \in R$ vrijedi: $f + g, r \cdot g$ i $f * g \in I(X, R)$. Zatvorenost na konvoluciju funkcija slijedi iz tranzitivnosti od $\leq$, naime za $x, y, z \in X$, $x \not\leq y$ vrijedi:

$$\begin{aligned} x \leq z \Rightarrow z \not\leq y \Rightarrow g(z, y) = 0 \Rightarrow (f * g)(x, y) = 0, \\ z \leq y \Rightarrow x \not\leq z \Rightarrow f(x, z) = 0 \Rightarrow (f * g)(x, y) = 0. \end{aligned}$$

Prisjetimo se definicije R-modula i asocijativne R-algebre s jedinicom.

Definicija 2.8. *Neka je $R = (R, +, \cdot)$ prsten s jedinicom.* ***Lijevi R-modul*** *ili* ***lijevi modul nad*** *R je komutativna grupa $M = (M, +)$ zajedno s preslikavanjem $R \times M \ni (r, m) \mapsto r \cdot m \in M$ koje zadovoljava:*

i) $\forall m \in M: \quad 1 \cdot m = m,$

ii) $\forall m, n \in M,\ r \in R: \quad r \cdot (m + n) = r \cdot m + r \cdot n,$

iii) $\forall m \in M,\ r, s \in R: \quad (r + s) \cdot m = r \cdot m + s \cdot m,$

iv) $\forall m \in M,\ r, s \in R: \quad r \cdot (s \cdot m) = (r \cdot s) \cdot m.$

Pojam desnog R-modula definira se analogno kao u definiciji 2.8. Ukoliko je R komutativan prsten, pojmovi lijevog i desnog R-modula se podudaraju pa jednostavno kažemo R-modul.

Definicija 2.9. *Neka je $M = (M, +, \cdot)$ modul nad komutativnim prstenom s jedinicom R. Ako je M snabdjeven dodatnom operacijom množenja $M \times M \ni (x, y) \mapsto x \cdot y \in M$ koja je bilinearna, asocijativna i postoji jedinstveni element $1_M \in M$ koji zadovoljava $1_M \cdot x = x \cdot 1_M = x$ za sve $x \in M$, onda za M kažemo da je* ***asocijativna R-algebra s jedinicom****.*

Za operaciju množenja iz definicije 2.9 kažemo da je bilinerana ako zadovoljava $(\alpha x_1+\beta x_2)\cdot y = \alpha(x_1\cdot y)+\beta(x_2\cdot y)$ i $x\cdot(\alpha y_1+\beta y_2) = \alpha(x\cdot y_1)+\beta(x\cdot y_2)$ za $\alpha, \beta \in R,\ x_1, x_2, y_1, y_2, x, y \in M$.

Uvedimo sada neke važne funkcije u incidencijsku algebru $I(X, R)$. Ako je A podskup od X, definiramo funkciju $\delta_A \in I(X, R)$ s:

$$\delta_A(x, y) = \begin{cases} 1, & \text{ako je } x = y \in A, \\ 0, & \text{inače.} \end{cases}$$

Ako je $A = X$, onda pišemo $\delta_X = \delta$ i funkciju δ zovemo Kroneckerovom funkcijom. Dodatno, definiramo $\delta_{xy} \in I(X, R)$ s:

$$\delta_{xy}(u, v) = \begin{cases} 1, & \text{ako je } u = x \text{ i } v = y, \\ 0, & \text{inače} \end{cases}$$

i pišemo e_x za δ_{xx}.

Sljedeće, definiramo funkciju $\chi \in I(X, R)$ s:

$$\chi(x, y) = \begin{cases} 1, & \text{ako je } x < y, \\ 0, & \text{inače,} \end{cases} \tag{1}$$

pritom $x < y$ znači $x \leq y$ i $x \neq y$. Na $I(X, R)$ definiramo i tzv. *zeta funkciju* s: $\zeta = \delta + \chi$.

Neutralni element za množenje u incidencijskoj algebri $I(X, R)$ je funkcija $\delta \in I(X, R)$. Zaista, vrijedi:

$$(f * \delta)(x, y) = \sum_{x \leq z \leq y} f(x, z) \cdot \delta(z, y) = f(x, y)$$

i

$$(\delta * f)(x, y) = \sum_{x \leq z \leq y} \delta(x, z) \cdot f(z, y) = f(x, y)$$

Teorem 2.10. *$I(X, R)$ je asocijativna R-algebra s jedinicom.*

Dokaz. $(I(X, R), +)$ je komutativna grupa. Zbrajanje u incidencijskoj algebri $I(X, R)$ je definirano po točkama pa asocijativnost i komutativnost očito vrijede. Neutralni element je funkcija $f \equiv 0$, a suprotni element od f je funkcija $-f$. Nadalje, $(I(X, R), +, \cdot)$ je R-modul jer množenje skalarom zadovoljava pretpostavke iz definicije 2.8, to jest za sve $x, y \in X$ vrijedi:

i) $1 \cdot f(x, y) = f(x, y), \quad \forall f \in I(X, R),$

ii) $r \cdot (f(x,y)+g(x,y)) = r \cdot f(x,y) + r \cdot g(x,y), \quad \forall f, g \in I(X,R),\ r \in R,$

iii) $(r+s) \cdot f(x,y) = r \cdot f(x,y) + s \cdot f(x,y), \quad \forall f \in I(X,R),\ r, s \in R,$

iv) $r \cdot (s \cdot f(x,y)) = (r \cdot s) \cdot f(x,y), \quad \forall f \in I(X,R),\ r, s \in R.$

Neutralni element za množenje u $I(X,R)$ je Kroneckerova δ funkcija. Pokažimo sada bilinearnost množenja.

$$\begin{aligned}
((\alpha f_1 + \beta f_2) * g)(x,y) &= \sum_{x \le z \le y} (\alpha f_1 + \beta f_2)(x,z) \cdot g(z,y) \\
&= \sum_{x \le z \le y} (\alpha f_1(x,z) + \beta f_2(x,z)) \cdot g(z,y) \\
&= \sum_{x \le z \le y} \alpha f_1(x,z) g(z,y) + \beta f_2(x,z) g(z,y) \\
&= \alpha \sum_{x \le z \le y} f_1(x,z) g(z,y) + \beta \sum_{x \le z \le y} f_2(x,z) g(z,y) \\
&= \alpha (f_1 * g)(x,y) + \beta (f_2 * g)(x,y)
\end{aligned}$$

za $x, y \in X,\ f_1, f_2, g \in I(X,R)$. Slično se pokaže da vrijedi i

$$g * (\alpha f_1 + \beta f_2)(x,y) = \alpha (g * f_1)(x,y) + \beta (g * f_2)(x,y).$$

Preostaje nam još pokazati asocijativnost množenja. Naime, za $x, y \in X$ te $f, g, h \in I(X,R)$ vrijedi:

$$\begin{aligned}
((f * g) * h)(x,y) &= \sum_{x \le z \le y} (f * g)(x,z) \cdot h(z,y) \\
&= \sum_{x \le z \le y} \left(\sum_{x \le w \le z} f(x,w) g(w,z) \right) \cdot h(z,y) \\
&= \sum_{x \le z \le y} \sum_{x \le w \le z} f(x,w) g(w,z) h(z,y) \\
&= \sum_{x \le z \le y} \sum_{x \le w \le y} f(x,w) g(w,z) h(z,y) \\
&= \sum_{x \le w \le y} \sum_{x \le z \le y} f(x,w) g(w,z) h(z,y) \\
&= \sum_{x \le w \le y} f(x,w) \left(\sum_{w \le z \le y} g(w,z) h(z,y) \right) \\
&= \sum_{x \le w \le y} f(x,w) \cdot (g * h)(w,y) \\
&= (f * (g * h))(x,y).
\end{aligned}$$

U četvrtoj jednakosti koristili smo činjenicu da je $g(w,z) = 0$ za $w \not\leq z$ pa indeks w može ići do y. U petoj jednakosti koristili smo zamjenu poretka sumacije. U šestoj jednakosti vrijednost $f(x,w)$ ne ovisi o indeksu z pa koristeći svojstvo distributivnosti može izaći ispred druge sume. Također, u šestoj jednakosti vrijedi $g(w,z) = 0$ za $w \not\leq z$ pa indeks z može ići od w do y. Korištenjem definicije konvolucije funkcija u $I(X,R)$ u posljednje dvije jednakosti slijedi tvrdnja. □

Sljedeći teorem pomoći će nam u određivanju invertibilnih funkcija u $I(X,R)$.

Teorem 2.11. *Neka je X lokalno konačan parcijalno uređen skup i R komutativni prsten s jedinicom. Za $f \in I(X,R)$ slijedeće tvrdnje su ekvivalentne:*

(a) f ima desni inverz,

(b) f ima lijevi inverz,

(c) f je invertibilni element,

(d) $f(x,x)$ je invertibilni element prstena R za svaki $x \in X$.

Dokaz. Pokazat ćemo ekvivalenciju (a) i (d). Ekvivalencija (b) i (d) slijedi sličnim argumentiranjem. S obzirom da (d) povlači i (a) i (b), iz leme 2.6 slijedi da (d) povlači (c). Konačno, kako (c) očito povlači (a) i (b) teorem će biti dokazan.

(a) $\Longrightarrow$ (d) Pretpostavimo da f ima desni inverz g, tada za svaki $x \in X$ imamo $(f * g)(x,x) = f(x,x) \cdot g(x,x) = \delta(x,x) = 1$ i $f(x,x)$ je invertibilni element prstena R.

(d) $\Longrightarrow$ (a) Pretpostavimo da je $f(x,x)$ invertibilni element prstena R za svaki $x \in X$. Definiramo desni inverz g induktivno po kardinalitetu segmenta u X. Ako je $|[x,y]| = 0$, onda je $x \not\leq y$ i stavljamo $g(x,y) = 0$. Ako je $|[x,y]| = 1$, onda je $x = y$ i stavljamo $g(x,x) = (f(x,x))^{-1}$. Neka je $n > 1$ i pretpostavimo da je za svaki segment kardinaliteta manjeg od n funkcija g definirana na tom segmentu. Neka je $[x,y]$ segment kardinaliteta n. Želimo

$$\begin{aligned} 0 &= (f * g)(x,y) \\ &= \sum_{x \leq z \leq y} f(x,z) \cdot g(z,y) \\ &= f(x,x) \cdot g(x,y) + \sum_{x < z \leq y} f(x,z) \cdot g(z,y). \end{aligned}$$

S obzirom da je $f(x,x)$ invertibilan, možemo riješiti ovu jednadžbu po $g(x,y)$ pa definiramo

$$g(x,y) = \left(- \sum_{x<z\leq y} f(x,z) \cdot g(z,y) \right) \cdot f(x,x)^{-1}.$$

Segmenti $[z,y]$ imaju kardinalitet manji od n pa je po pretpostavci indukcije funkcija g definirana na tim segmentima. Dakle, $f * g = \delta$. □

Množenje elemenata u incidencijskoj algebri usko je povezano s matričnim množenjem. Sa $M_n(R)$ označimo skup $n \times n$ matrica gdje je R komutativni prsten s jedinicom. Dodatno, sa $T_n(R)$ označimo skup svih $n \times n$ gornjetrokutastih matrica te sa $L_n(R)$ skup svih $n \times n$ donjetrokutastih matrica. $M_n(R), T_n(R)$ i $L_n(R)$ su asocijativne R-algebre s jedinicom. Za dokazivanje tvrdnje o ulaganju incidencijske algebre $I(X,R)$ u algebre $T_n(R)$ i $L_n(R)$ trebat će nam posebno indeksiranje elemenata parcijalno uređenog skupa koje pokazujemo u sljedećoj lemi. Za element x parcijalno uređenog skupa X kažemo da je *maksimalan* ako vrijedi $x = y$ kadgod je $x \leq y$.

Lema 2.12. *Konačan parcijalno uređen skup $(X, \leq)$ može se označiti s $X = \{x_1, \ldots, x_n\}$ tako da $x_i \leq x_j$ povlači $i \leq j$.*

Dokaz. Tvrdnju ćemo dokazati indukcijom po kardinalitetu skupa X. Ako je X jednočlan skup, tvrdnja očito vrijedi. Za $n > 1$ pretpostavimo da se svaki parcijalno uređeni skup kardinaliteta manjeg od n može označiti kao u tvrdnji leme. Neka je sada X parcijalno uređen skup kardinaliteta n. Kako je X konačan znamo da ima maksimalni element pa ga označimo s x_n. Podskup $X \setminus \{x_n\}$ ima kardinalitet manji od n pa po pretpostavci indukcije za njega vrijedi tvrdnja, to jest skup $X \setminus \{x_n\}$ možemo označiti s $X \setminus \{x_n\} = \{x_1, \ldots, x_{n-1}\}$ tako da $x_i \leq x_j$ povlači $i \leq j$. Dodavanjem elementa x_n u skup $X \setminus \{x_n\}$ imamo $X = \{x_1, \ldots, x_n\}$. Zbog maksimalnosti od x_n vrijedi da $x_i \leq x_n$ povlači $i \leq n$, $i \in \{1, \ldots, n\}$. □

Slično kao u prethodnoj lemi, elementi konačnog parcijalno uređenog skupa $X = \{x_1, \ldots, x_n\}$ mogu se indeksirati tako da $x_i \geq x_j$ povlači $i \leq j$. Pokažimo sada spomenuto ulaganje incidencijske algebre u algebru gornjetrokutastih i donjetrokutastih matrica.

Propozicija 2.13. *Neka je $X = \{x_1, \ldots, x_n\}$ parcijalno uređen skup i R komutativan prsten s jedinicom.*

(a) Incidencijska algebra $I(X,R)$ izomorfna je podalgebri od $T_n(R)$.

(b) Incidencijska algebra $I(X,R)$ izomorfna je podalgebri od $L_n(R)$.

Dokaz. Dokažimo tvrdnju (a). Neka je $X = \{x_1, \ldots, x_n\}$ indeksiran kao u lemi 2.12. Definirajmo preslikavanje $\Psi\colon I(X,R) \to T_n(R)$ s:

$$\Psi(f)(i,j) = f(x_i, x_j)$$

za $f \in I(X,R)$, $i,j \in \{1,\ldots,n\}$. Ovako definirano preslikavanje svakoj funkciji $f \in I(X,R)$ pridružuje matricu $A = [a_{ij}], a_{ij} = f(x_i,x_j)$. Matrica A je gornjetrokutasta, a preslikavanje Ψ je injektivni homomorfizam. Ako $f \overset{\Psi}{\mapsto} A$ i $g \overset{\Psi}{\mapsto} B$, vrijedi

$$\begin{aligned}(f*g)(x_i,x_j) &= \sum_{x_k \in [x_i,x_j]} f(x_i,x_k)\cdot g(x_k,x_j) = \sum_{x_k\in[x_i,x_j]} a_{ik}\cdot b_{kj} = \sum_{i\le k\le j} a_{ik}\cdot b_{kj} \\ &= \sum_{k=1}^{n} a_{ik}\cdot b_{kj} = (A\cdot B)_{ij}.\end{aligned}$$

U trećem koraku sumirali smo po svim indeksima k koji zadovoljavaju $i \le k \le j$ jer za $x_i \not\leq x_k$ je $a_{ik} = 0$, a za $x_k \not\leq x_j$ je $b_{kj} = 0$ pa se suma ne mijenja. Slično, u četvrtom koraku sumu smo proširili na sve indekse od 1 do n jer je $a_{ik} = 0$ za $k < i$ te $b_{kj} = 0$ za $k > j$. Dakle, vrijedi $(f*g) \overset{\Psi}{\mapsto} A\cdot B$, odnosno Ψ čuva množenje. Preslikavanje Ψ je monomorfizam algebri, a njegova slika je podalgebra od $T_n(R)$ izomorfna incidencijskoj algebri $I(X,R)$. Tvrdnja (b) dokazuje se slično kao tvrdnja (a) indeksiranjem skupa X tako da $x_i \ge x_j$ povlači $i \le j$. □

Lema 2.12 može se proširiti na slučaj kad je X prebrojiv skup.

Lema 2.14. *Elementi prebrojivog parcijalno uređenog skupa $(X,\le)$ mogu se indeksirati racionalnim brojevima tako da $x_i \le x_j$ povlači $i \le j$.*

Dokaz. Neka je $X = \{y_1, y_2, \ldots\}$. Definirajmo preslikavanje $\psi\colon X \to \mathbb{Q}$ na sljedeći način. Neka je $\psi(y_1) = 1$. Ako je $y_2 < y_1$, onda definiramo $\psi(y_2) = 0$, inače definiramo $\psi(y_2) = 2$. Pretpostavimo da ψ pridružuje racionalan broj svakom $y_k \in X$ za $1 \le k < n$ sa svojstvom da $y_i \le y_j$ povlači $\psi(y_i) \le \psi(y_j)$, $i,j \in \{1,\ldots,n-1\}$. Promotrimo sada element $y_n \in X$. Označimo s $Y_< = \{y \in X\colon y < y_n\}$ te s $Y_> = \{y \in X\colon y > y_n\}$. Za $y_i \in Y_<$ i $y_j \in Y_>$ vrijedi $y_i < y_n$ i $y_n < y_j$ pa zbog tranzitivnosti parcijalnog uređaja $\le$ vrijedi $y_i < y_j$. Po pretpostavci vrijedi $\psi(y_i) < \psi(y_j)$ za sve $y_i \in Y_<, y_j \in Y_>$. Skup $\psi_< = \{q \in \mathbb{Q} \mid \psi(y_i) = q, y_i \in Y_<\}$ je odozgo omeđen pa postoji supremum, označimo ga s $q_<$. Skup $\psi_> = \{q \in \mathbb{Q} \mid \psi(y_j) = q, y_j \in Y_>\}$ je odozdo omeđen pa postoji infimum, označimo ga s $q_>$. Sada možemo izabrati

broj $q_n = \frac{q_< + q_>}{2}$ i definirati $\psi(y_n) = q_n$. Za $\{y_1, \ldots, y_n\}$ vrijedi da $y_i \leq y_j$ povlači $\psi(y_i) \leq \psi(y_j)$ za $i, j \in \{1, \ldots, n\}$. Nastavljajući na ovaj način, sve elemente skupa X možemo indeksirati s $x_{\psi(y_i)} = y_i$. □

Promotrimo ponovno parcijalno uređene skupove iz primjera 2.4 te odredimo njihove incidencijske algebre, odnosno matrice koje one sadrže. Neka je R komutativni prsten s jedinicom.

Primjer 2.15. *1) Promotrimo podskup od* $(\mathbb{R}, \leq)$ *s prirodnim uređajem* $(\{1,2,3\}, \leq)$. *Incidencijska algebra od parcijalno uređenog skupa* $(\{1,2,3\}, \leq)$ *izomorfna je podalgebri od* $T_3(R)$, *a izomorfizam izgleda ovako:*

$$I(\{1,2,3\}, R) \to \begin{pmatrix} R & R & R \\ 0 & R & R \\ 0 & 0 & R \end{pmatrix}$$

Pritom se u matrici na nenul mjestima nalazi neki element prstena R.

2) Za antilanac $A = \{\{1\}, \{2\}, \{3\}\}$ *parcijalno uređenog skupa* $(\mathcal{P}(\{1,2,3\}), \subseteq)$ *vrijedi:*

$$I(A, R) \to \begin{pmatrix} R & 0 & 0 \\ 0 & R & 0 \\ 0 & 0 & R \end{pmatrix}$$

3) Za parcijalno uređen skup $(\mathbb{N}, |)$ *imamo:*

$$I((\mathbb{N}, |), R) \to \begin{pmatrix} R & R & R & R & R & R & \ldots \\ 0 & R & 0 & R & 0 & R & \ldots \\ 0 & 0 & R & 0 & 0 & R & \ldots \\ 0 & 0 & 0 & R & 0 & 0 & \ldots \\ 0 & 0 & 0 & 0 & R & 0 & \ldots \\ 0 & 0 & 0 & 0 & 0 & R & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

4) Ako uzmemo $S = \{1,2\}$ *te promotrimo* $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$ *imamo:*

$$I((\mathcal{P}(S), \subseteq), R) \to \begin{pmatrix} R & R & R & R \\ 0 & R & 0 & R \\ 0 & 0 & R & R \\ 0 & 0 & 0 & R \end{pmatrix}$$

3 Möbiusova inverzija

Incidencijske algebre razvile su se kao prirodno okruženje za generalizaciju formule Möbiusove inverzije u teoriji brojeva. Generalizirana formula Möbiusove inverzije s kojom ćmo se upoznati u ovom poglavlju ima važnu kombinatornu primjenu. Njemački matematičar i astronom A.F. Möbius definirao je funkciju μ s

$$\mu(n) = \begin{cases} 0, & \text{ako je } n \text{ djeljiv s kvadratom prostog broja,} \\ (-1)^k, & \text{ako je } n \text{ produkt } k \text{ različitih prostih brojeva,} \\ 1, & n = 1. \end{cases}$$

Prethodnu definiranu funkciju zovemo *klasičnom Möbiusovom funkcijom*. Prije generalizacije, iskažimo teorem klasične Möbiusove inverzije.

Teorem 3.1. *Neka su $f, g\colon \mathbb{N} \to R$ pri čemu je R komutativni prsten s jedinicom te μ klasična Möbiusova funkcija. Ekvivalentno je*

(a) $g(n) = \sum_{d|n} f(d)$ *i*

(b) $f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$.

Neka je $(X, \leq)$ lokalno konačan parcijalno uređen skup te R komutativni prsten s jedinicom. Prisjetimo se zeta funkcije u incidencijskoj algebri $I(X, R)$ iz prethodnog poglavlja:

$$\zeta(x, y) = \begin{cases} 1, & \text{ako je } x \leq y, \\ 0, & \text{inače.} \end{cases}$$

Pokažimo najprije da zeta funkcija ima inverz u $I(X, R)$.

Propozicija 3.2. *Zeta funkcija lokalno konačnog parcijalno uređenog skupa $(X, \leq)$ je invertibilna u $I(X, R)$.*

Dokaz. Po teoremu 2.11 dovoljno je pokazati da je $\zeta(x, x)$ invertibilni element prstena R za svaki $x \in X$. Naime, $\zeta(x, x) = 1$ pa tvrdnja vrijedi. □

Sada možemo definirati inverz $\mu(x, y)$ zeta funkcije za $x, y \in X$ induktivno po kardinalitetu segmenta $[x, y]$ kao u dokazu teorema 2.11.

$$\mu(x, y) = \begin{cases} 1, & \text{ako } x = y, \\ -\sum_{x < z \leq y} \mu(z, y), & \text{ako } x < y, \\ 0, & \text{inače.} \end{cases}$$

Ovako definiran inverz zeta funkcije nazivamo *Möbiusovom funkcijom* incidencijske algebre $I(X, R)$.

Definicija 3.3. *Neka je x element lokalno konačnog parcijalno uređenog skupa X. Skup $I_x = \{y \in X \mid y \leq x\}$ je* ***glavni ideal skupa*** *X* ***generiran s*** *x, a skup $U_x = \{y \in X \mid y \geq x\}$ je* ***glavni filter skupa*** *X* ***generiran s*** *x.*

U sljedeća dva teorema navodimo generalizirane formule Möbiusove inverzije.

Teorem 3.4. *Neka je X lokalno konačan parcijalno uređen skup, R komutativni prsten s jedinicom i $f\colon X \to R$ funkcija. Pretpostavimo da je za svaki $x \in X$ glavni filter generiran s x konačan. Ako je $g(x) = \sum_{x \leq y} f(y)$, onda je $f(x) = \sum_{x \leq y} \mu(x, y) \cdot g(y)$.*

Dokaz.

$$\begin{aligned}
\sum_{x \leq y} \mu(x,y) \cdot g(y) &= \sum_{x \leq y} \mu(x,y) \cdot \sum_{y \leq z} f(z) \\
&= \sum_{x \leq y} \mu(x,y) \cdot \sum_{y \leq z} \zeta(y,z) \cdot f(z) \\
&= \sum_{x \leq y} \sum_{y \leq z} \mu(x,y) \cdot \zeta(y,z) \cdot f(z) \\
&= \sum_{y \leq z} \sum_{x \leq y} \mu(x,y) \cdot \zeta(y,z) \cdot f(z) \\
&= \sum_{y \leq z} \left(\sum_{x \leq y} \mu(x,y) \cdot \zeta(y,z) \right) f(z) \\
&= \sum_{x \leq y \leq z} \delta(x,z) \cdot f(z) = f(x)
\end{aligned}$$

□

Slično kao za prethodni teorem pokaže se da vrijedi sljedeće.

Teorem 3.5. *Neka je X lokalno konačan parcijalno uređen skup, R komutativni prsten s jedinicom i $f\colon X \to R$ funkcija. Pretpostavimo da je za svaki $x \in X$ glavni ideal generiran s x konačan. Ako je $g(x) = \sum_{y \leq x} f(y)$, onda je $f(x) = \sum_{y \leq x} g(y) \cdot \mu(y, x)$.*

U mnogim primjenama Möbiusove inverzije nužno je znati vrijednosti Möbiusove funkcije μ na elementima parcijalno uređenog skupa. Sada ćemo dati nekoliko važnih svojstava koja će nam pomoći u računanju. Najvažnije svojstvo Möbiusove funkcije μ je da je ona inverzna funkcija zeta funkciji iz čega slijedi sljedeća propozicija.

Propozicija 3.6. *Neka je X lokalno konačan parcijalno uređen skup, R komutativni prsten s jedinicom i $\mu \in I(X, R)$ Möbiusova funkcija. Tada vrijedi*

(a) $\mu(x, x) = 1$ za sve $x \in X$,

(b) za različite $x, y \in X$ vrijedi jednakost $\sum_{x \leq z \leq y} \mu(x, z) = 0$,

(c) za različite $x, y \in X$ vrijedi jednakost $\sum_{x \leq z \leq y} \mu(z, y) = 0$ i

(d) $\mu(x, y)$ je cijeli broj u prstenu R za sve $x, y \in X$.

Dokaz. Tvrdnje (a), (b) i (c) slijede iz jednakosti

$$\delta(x, y) = (\mu * \zeta)(x, y) = (\zeta * \mu)(x, y).$$

Naime, za sve $x \in X$ vrijedi

$$\begin{aligned} \delta(x, x) &= \mu(x, x) \cdot \zeta(x, x) \\ 1 &= \mu(x, x) \cdot 1 \end{aligned}$$

iz čega slijedi (a).

Za $x \neq y \in X$ vrijedi $\delta(x, y) = 0$ pa iz

$$\delta(x, y) = \sum_{x \leq z \leq y} \mu(x, z) \cdot \zeta(z, y)$$

i

$$\delta(x, y) = \sum_{x \leq z \leq y} \zeta(x, z) \cdot \mu(z, y)$$

slijede (b) i (c). Cijeli brojevi u prstenu R su elementi potprstena generiranog s jedinicom prstena R pa tvrdnja (d) slijedi iz definicije funkcije μ. Naime, zeta funkcija poprima vrijednosti 0 i 1, a vrijednosti Möbiusove funkcije kao inverza od zeta funkcije se po teoremu 2.11 dobije zbrajanjem, oduzimanjem i množenjem vrijednosti od ζ i prethodnih vrijednosti od μ te dijeljenjem sa $\zeta(x, x) = 1$. □

Prethodna propozicija pokazuje da Möbiusova funkcija incidencijske algebre $I(X, R)$ ovisi samo o parcijalno uređenom skupu X, ne i o prstenu R karakteristike 0. Posljedica prethodne propozicije govori nam o tome da se kod računanja $\mu(x, y)$ možemo ograničiti samo na konačan parcijalno uređen skup $[x, y]$.

Korolar 3.7. *Neka je X lokalno konačan parcijalno uređen skup te $x, y \in X$. Tada je $\mu_X(x, y) = \mu_{[x,y]}(x, y)$.*

Dokaz. Indukcijom po kardinalitetu segmenta $[x, y]$ i korištenjem propozicije 3.6 možemo vidjeti da se vrijednost Möbiusove funkcije u (x, y) na X podudara s vrijednošću Möbiusove funkcije u (x, y) na $[x, y]$. □

Iz definicije funkcije χ iz prethodnog poglavlja lako se vidi da $\chi^n(x, y)$ daje broj različitih lanaca od x do y duljine $n+1$ u segmentu $[x, y]$. Također vrijedi $\zeta = \delta + \chi$.

Korolar 3.8. *Neka je X lokalno konačan parcijalno uređen skup te $x, y \in X$. Neka je $C_n(x, y)$ skup svih lanaca duljine n od x do y u X pri čemu je n pozitivan cijeli broj. Tada vrijedi*

$$\mu(x, y) = |C_1(x, y)| - |C_2(x, y)| + |C_3(x, y)| - |C_4(x, y)| + \dots$$

Dokaz. Po korolaru 3.7 bez smanjenja općenitosti možemo pretpostaviti da vrijedi $X = [x, y]$. Tada

$$\mu = \zeta^{-1} = (\delta + \chi)^{-1} = \delta - \chi + \chi^2 - \chi^3 + \dots$$

S obzirom na to da je $[x, y]$ konačan, $\chi^n = 0$ za dovoljno velik n. Iz $\chi^r(x, y) = |C_{r+1}(x, y)|$ slijedi tvrdnja. □

Za parcijalno uređen skup X ćemo s 0 označiti najmanji element, to jest element za kojeg vrijedi $0 \leq x$, $\forall x \in X$, ukoliko takav postoji. Analogno, s 1 ćemo označiti najveći element, to jest element za kojeg vrijedi $x \leq 1$, $\forall x \in X$. Svaki lokalno konačan parcijalno uređen skup X s 0 i 1 je konačan jer je segment $X = [0, 1]$ po definiciji 2.2 konačan.

Sljedeća propozicija nam daje induktivnu metodu za računanje vrijednosti $\mu(0, 1)$ za parcijalno uređene skupove s 0 i 1.

Propozicija 3.9. *Neka je X konačan parcijalno uređen skup s 0 i 1 te $x_0 \in X \backslash \{0, 1\}$. Tada je $\mu_X(0, 1) = \mu_{X\backslash\{x_0\}}(0, 1) + \mu_X(0, x_0) \cdot \mu_X(x_0, 1)$.*

Dokaz. Neka je C_n skup svih lanaca od 0 do 1 u X duljine n. Nadalje, označimo s D_n lance iz C_n koji ne sadrže x_0 te s $E_n = C_n \backslash D_n$. Iz korolara 3.8 slijedi

$$\mu_{X\backslash\{x_0\}}(0,1) = |D_1| - |D_2| + |D_3| - |D_4| + \dots$$

Neka je $\alpha \in E_n$. Tada za neki pozitivan cijeli broj j, lanac α možemo podijeliti na lanac β od 0 do x_0 duljine j te lanac γ od x_0 do 1 duljine $n - j + 1$. U alternirajućoj sumi izraza $\mu(0, x_0)$ lanac β doprinosi $(-1)^{j-1}$, dok u alternirajućoj sumi izraza $\mu(x_0, 1)$ lanac γ doprinosi $(-1)^{n-j}$. Umnožak ovih doprinosa podudara se s doprinosom od α u alternirajućoj sumi od $\mu(0, 1)$. □

Prije uspoređivanja Möbiusovih funkcija izomorfnih i anti-izomorfnih parijalno uređenih skupova navedimo definiciju.

Definicija 3.10. *Neka su $(X, \leq_X)$ i $(Y, \leq_Y)$ parcijalno uređeni skupovi te $\rho\colon X \to Y$ bijekcija.*

i) Ako ρ ima svojstvo da vrijedi $x_1 \leq_X x_2$ ako i samo ako vrijedi $\rho(x_1) \leq_Y \rho(x_2)$, onda je ρ ***izomorfizam parcijalno uređenih skupova****.*

ii) Ako ρ ima svojstvo da vrijedi $x_1 \leq_X x_2$ ako i samo ako vrijedi $\rho(x_2) \leq_Y \rho(x_1)$, onda je ρ ***anti-izomorfizam parcijalno uređenih skupova****.*

Propozicija 3.11. *Pretpostavimo da su $(X, \leq_X)$ i $(Y, \leq_Y)$ lokalno konačni parcijalno uređeni skupovi te $\rho\colon X \to Y$ bijekcija. Neka su $x_1, x_2 \in X$.*

(a) Ako je ρ izomorfizam parcijalno uređenih skupova, onda je

$$\mu_X(x_1, x_2) = \mu_Y(\rho(x_1), \rho(x_2)).$$

(b) Ako je ρ anti-izomorfizam parcijalno uređenih skupova, onda je

$$\mu_X(x_1, x_2) = \mu_Y(\rho(x_2), \rho(x_1)).$$

Dokaz. Dokaz slijedi iz prethodne definicije te odgovarajućih relacija za zeta funkciju. □

Mnogi parcijalno uređeni skupovi koji se koriste u kombinatornim primjenama izomorfni su direktnom produktu jedostavnijih parcijalno uređnih skupova. Kad je parcijalno uređen skup Z direktan produkt parcijalno uređenih skupova X i Y, onda se Möbiusova funkcija od Z može lako dobiti iz Möbiusovih funkcija od X i Y. Definirajmo najprije direktan produkt parcijalno uređenih skupova.

Definicija 3.12. *Neka su $(X, \leq_X)$ i $(Y, \leq_Y)$ parcijalno uređeni skupovi. Parcijalno uređen skup $Z = (X \times Y, \leq_Z)$ s parcijalnim uređajem $\leq_Z$ definiranim s $(x_1, y_1) \leq_Z (x_2, y_2)$ ako i samo ako $x_1 \leq_X x_2$ i $y_1 \leq_Y y_2$ za $x_1, x_2 \in X,\ y_1, y_2 \in Y$ nazivamo* ***direktnim produktom*** *parcijalno uređenih skupova X i Y.*

Ako je $Z = (X \times Y, \leq_Z)$ direktan produkt lokalno konačnih parcijalno uređenih skupova $(X, \leq_X)$ i $(Y, \leq_Y)$, onda je i Z lokalno konačan. Vrijedi

$$\delta_Z((x_1, y_1), (x_2, y_2)) = \delta_X(x_1, x_2) \cdot \delta_Y(y_1, y_2)$$

i

$$\zeta_Z((x_1, y_1), (x_2, y_2)) = \zeta_X(x_1, x_2) \cdot \zeta_Y(y_1, y_2).$$

Slično vrijedi i za Möbiusovu funkciju od $X \times Y$.

Propozicija 3.13. *Neka su X i Y lokalno konačni parcijalno uređeni skupovi te $Z = (X \times Y, \leq_Z)$ njihov direktan produkt. Tada za $x_1, x_2 \in X$ te $y_1, y_2 \in Y$ vrijedi*

$$\mu_Z((x_1, y_1), (x_2, y_2)) = \mu_X(x_1, x_2) \cdot \mu_Y(y_1, y_2).$$

Dokaz. Neka je $f \in I(X \times Y, R)$ definirana s

$$f((x_1, y_1), (x_2, y_2)) = \mu_X(x_1, x_2) \cdot \mu_Y(y_1, y_2).$$

Pokazat ćemo da vrijedi $\zeta_Z * f = \delta_Z$.

$$\begin{aligned}
(\zeta_Z * f)((x_1, y_1), (x_2, y_2)) &= \sum_{(x_1,y_1) \leq (x,y) \leq (x_2,y_2)} \zeta_Z((x_1, y_1), (x, y)) \cdot f((x, y), (x_2, y_2)) \\
&= \sum_{(x_1,y_1) \leq (x,y) \leq (x_2,y_2)} \zeta_X(x_1, x) \cdot \zeta_Y(y_1, y) \cdot \mu_X(x, x_2) \cdot \mu_Y(y, y_2) \\
&= \sum_{\substack{x_1 \leq x \leq x_2, \\ y_1 \leq y \leq y_2}} \zeta_X(x_1, x) \cdot \mu_X(x, x_2) \cdot \zeta_Y(y_1, y) \cdot \mu_Y(y, y_2) \\
&= \delta_X(x_1, x_2) \cdot \delta_Y(y_1, y_2) \\
&= \delta_Z((x_1, y_1), (x_2, y_2)).
\end{aligned}$$

S obzirom na to da da je μ_Z inverz od ζ_Z slijedi $\mu_Z = f$. □

Izračunajmo sada Möbiusovu funkciju nekih parcijalno uređenih skupova.

Primjer 3.14. *Neka je C_n lanac koji se sastoji od cijelih brojeva 0 do $n-1$ sa standardnim uređajem $\leq$.*

Ako su $i, j \in C_n$, $i \leq j$, onda vrijedi $[i,j] \simeq C_{j-i+1}$. Odatle slijedi da je dovoljno izračunati $\mu(0,k)$ za $k \geq 0$. Ako je $k = 0$, onda imamo $\mu(0,0) = 1$. Ako je $k = 1$, po propoziciji 3.6 imamo $\mu(0,0) + \mu(0,1) = 0$ pa je $\mu(0,1) = -1$. Koristeći indukciju i propoziciju3.6 zaključujemo da vrijedi $\mu(0,k) = 0$ za $k \geq 2$. Konačno, imamo

$$\mu(i,j) = \begin{cases} 1, & \text{ako je } i = j, \\ -1 & \text{ako je } j = i+1, \\ 0, & \text{inače.} \end{cases}$$

U ovom parcijalno uređenom skupu, teorem Möbiusove inverzije nam govori da kadgod je $b_n = \sum_j a_j$, tada je $a_n = b_n - b_{n-1}$. Ako je C lanac nenegativnih cijelih brojeva poredanih na uobičajen način, onda je Möbiusova funkcija od C određena Möbiusovom funkcijom konačnih lanaca od C. Zaista, ako su $i, j \in C$ pri čemu je $i \leq j \leq (n-1)$, onda je $\mu_C(i,j) = \mu_{C_n}(i,j)$.

Neka je $A \subseteq X$ podskup parcijalno uređenog skupa. Za element $g \in X$ kažemo da je *gornja međa* od A ako vrijedi $a \leq g$, $\forall a \in A$. Element $s \in X$ je *supremum* od A ako je gornja međa od A i za svaku gornju među g od A vrijedi $s \leq g$. Ako postoji, supremum je jedinstven i označavamo ga $supA$. Dualno definiramo donju među i infimum skupa A. Parcijalno uređen skup zovemo *rešetkom* ako za sve $x, y \in X$ postoje supremum $x \vee y = sup\{x, y\}$ i infimum $x \wedge y = inf\{x, y\}$.

Primjer 3.15. *Neka je $S = \{s_1, s_2, \ldots, s_n\}$ i $B(S)$ kolekcija svih podskupova od S. Parcijalno uređen skup $(B(S), \subseteq)$ je rešetka koju zovemo* ***Booleovom rešetkom skupa S****.*

Ako su $U, V \in B(S)$, $U \subseteq V$, onda vrijedi $[U,V] \simeq [\emptyset, V \backslash U]$. Za određivanje Möbiusove funkcije od $B(S)$ dovoljno je izračunati $\mu(\emptyset, S)$. Ako je $|S| = 1$, onda vrijedi $B(S) \simeq C_2$ i $\mu(\emptyset, S) = -1$. Neka je $A_i = \{s_i\}$. Tada je $B(A_i) \simeq C_2$ i $B(S) \simeq B(A_1) \times \cdots \times B(A_n)$. Iz propozicije 3.13 zaključujemo da vrijedi $\mu(\emptyset, S) = (-1)^n$. Dakle, za $U, V \in B(S)$, $U \subseteq V$ vrijedi $\mu(U,V) = (-1)^{|V|-|U|}$.

Klasičan princip uključivanja-isključivanja dobije se iz Möbiusove inverzije od $B_n = B(\{1, \ldots, n\})$. Neka je A konačan skup te $K_1, K_2, \ldots, K_n$ podskupovi od A, $n \in \mathbb{N}$. Tražimo $\left| A \setminus \bigcup_{i=1}^{n} K_i \right|$. Za $U \in B_n$, označimo s $N(U)$ broj elemanata od A koji su u $K_j \backslash K_r$ za $j \in U, r \notin U$. Nadalje, neka

je $\hat{N}(U)$ *broj elemenata od* A *koji su u* K_j *za sve* $j \in U$*. Tada vrijedi*

$$\hat{N}(U) = \left| \bigcap_{j \in U} K_j \right|$$

i

$$\hat{N}(\emptyset) = \mid A \mid = \sum_{U \in B_n} N(U).$$

Iz formula Möbiusove inverzije dobivamo

$$N(\emptyset) = \sum_{U \in B_n} (-1)^n \cdot \left| \bigcap_{j \in U} K_j \right|.$$

Primjer 3.16. *Neka je* $(\mathbb{N}, |)$ *parcijalno uređen skup pri čemu je* $|$ *relacija djeljivosti.*

Ako su $n, m \in \mathbb{N}$ *takvi da* $n \mid m$*, onda vrijedi* $[n, m] \simeq [1, \frac{m}{n}]$*. Slično kao u prethodnim primjerima, dovoljno je izračunati* $\mu(1, n)$ *za sve* $n \in \mathbb{N}$*. Ako je* $n = 1$*, onda vrijedi* $\mu(1, 1) = 1$*. Pretpostavimo da je* $n > 1$*. Neka je* $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ *rastav broja* n *na proste faktore gdje su* e_i *pozitivni cijeli brojevi. Neka je* $D_i = [1, p_i^{e_i}]$ *za* $i = 1, 2, \ldots, r$*. Zbog jedinstvenosti faktorizacije segment* $[1, n]$ *je izomorfan direktnom produktu parcijalno uređenih skupova* D_i *za* $i = 1, 2, \ldots, r$*. Štoviše,* D_i *je izomorfan* C_{e_i+1}*, lancu s* $e_i = 1$ *elementom. Iz propozicije 3.13 i primjera 3.14 slijedi*

$$\mu(1, n) = \begin{cases} 1, & \text{ako } n = 1, \\ (-1)^r, & \text{ako } e_i = 1 \text{ za svaki } i, \\ 0, & \text{inače.} \end{cases}$$

Kad su parcijalno uređeni skupovi na neki način povezani, informacije o Möbiusovoj funkciji jednog skupa mogu se dobiti pomoću informacija o Möbiusovoj funkciji drugog skupa, primjerice ako je jedan parcijalno uređen skup direktan produkt drugih parcijalno uređenih skupova. Jedan manje očit odnos među Möbiusovim funkcijama dvaju parcijalno uređenih skupova događa se kad su parcijalno uređeni skupovi povezani Galoisovom vezom.

Definicija 3.17. *Neka su* $(X, \leq)$ *i* $(Y, \preceq)$ *parcijalo uređeni skupovi. Kažemo da preslikavanje* $f \colon X \to Y$ ***čuva uređaj*** *ako vrijedi*

$$\forall x_1, x_2 \in X, \quad x_1 \leq x_2 \Rightarrow f(x_1) \preceq f(x_2)$$

te ***mijenja uređaj*** *ako vrijedi*

$$\forall x_1, x_2 \in X, \quad x_1 \leq x_2 \Rightarrow f(x_1) \succeq f(x_2).$$

Definicija 3.18. ***Galoisova veza*** *između parcijalno uređenih skupova X i Y je par preslikavanja koja mijenjaju uređaj $\phi\colon X \to Y$ i $\psi\colon Y \to X$ takvi da vrijedi $\psi(\phi(x)) \geq x$ i $\phi(\psi(y)) \geq y$ za sve $x \in X, y \in Y$.*

Definicija 3.19. ***Operator zatvaranja*** *na parcijalno uređenom skupu X je preslikavanje koje čuva uređaj $\lambda\colon X \to Y$ takvo da za sve $x \in X$ vrijedi*

i) $\lambda(x) \geq x$ *i*

ii) $\lambda(\lambda(x)) = \lambda(x)$.

Kažemo da je $x \in X$ ***zatvoren*** *ako vrijedi $\lambda(x) = x$.*

Ako je $\{\phi, \psi\}$ Galoisova veza između parcijalno uređenih skupova X i Y, onda vrijedi $\phi \circ \psi \circ \phi = \phi$ i $\psi \circ \phi \circ \psi = \psi$. Naime, neka je $x \in X,\ y \in Y$. Tada vrijedi

$$\psi(\phi(x)) \geq x \ /\phi$$
$$\phi(\psi(\phi(x)) \leq \phi(x)$$

i

$$\phi(\psi(\phi(x))) \geq \phi(x),$$

pri čemu prethodna nejednakost vrijedi iz definicije Galoisove veze za $\phi(x) \in Y$. Jednakost $\psi \circ \phi \circ \psi = \psi$ slijedi analogno. Iz prethodnog slijedi da je $\lambda_1 = \psi \circ \phi$ operator zatvaranja na X te $\lambda_2 = \phi \circ \psi$ operator zatvaranja na Y.

Ako je X lokalno konačan parcijalno uređen skup te $\lambda\colon X \to Y$ operator zatvaranja na X, pišemo $\overline{x}$ za $\lambda(x)$ te $\overline{X}$ za $\lambda(X)$, to jest $\overline{X}$ označava podskup elemenata od X koji su zatvoreni s obzirom na λ. Sljedeća propozicija nam daje vezu između Möbiusove funkcije od X i $\overline{X}$.

Propozicija 3.20. *Neka su y i z elementi lokalno konačnog parcijalno uređenog skupa X. Neka je $\overline{X}$ podskup od X koji sadrži sve elemente od X koji su zatvoreni. Tada*

$$\sum_{\overline{x}=\overline{z}} \mu(y, x) = \begin{cases} \mu_{\overline{X}}(y, \overline{z}), & \text{ako je } y \in \overline{X}, \\ 0, & \text{inače.} \end{cases}$$

Dokaz. Imamo

$$\begin{aligned}\sum_{\overline{x}=\overline{z}} \mu(y,x) &= \sum_{x\in X} \mu(y,x)\cdot\delta_{\overline{X}}(\overline{x},\overline{z}) \\ &= \sum_{\substack{x\in X\\ \overline{u}\in\overline{X}}} \mu(y,x)\cdot\zeta_{\overline{X}}(\overline{x},\overline{u})\cdot\mu_{\overline{X}}(\overline{u},\overline{z}) \\ &= \sum_{\substack{x\in X\\ \overline{u}\in\overline{X}}} \mu(y,x)\cdot\zeta(x,\overline{u})\cdot\mu_{\overline{X}}(\overline{u},\overline{z}) \\ &= \sum_{\overline{u}\in\overline{X}} \delta(y,\overline{u})\cdot\mu_{\overline{X}}(\overline{u},\overline{z}).\end{aligned}$$

S obzirom da je $\delta(y,\overline{u}) = 0$ osim u slučaju kad je $y \in \overline{X}$ te $y = \overline{u}$, tvrdnja slijedi. □

Korolar 3.21. *Neka su X i Y lokalno konačni parcijalno uređeni skupovi, preslikavanja $\phi\colon X \to Y$ i $\psi\colon Y \to X$ Galoisove veze te $\overline{X}$ podskup od X koji sadrži elemente od X zatvorene s obzirom na operator $\psi\circ\phi$. Tada za $z \in X$ i $w \in Y$ vrijedi*

$$\sum_{\phi(x)=w} \mu_X(z,x) = \sum_{\psi(y)=z} \mu_Y(w,y) = \mu_{\overline{X}}(z,\psi(w)).$$

Dokaz. Svaki izraz u prethodnoj jednakosti je jednak 0 osim ako su z i w zatvoreni. Ako su z i w zatvoreni, rezultat slijedi iz propozicije 3.20. □

Postoji veza između Möbiusove inverzije i algebarske topologije kao što je sugerirano u korolaru 3.8. Sada ćemo istražiti mali dio te veze. Ako je S konačan n-člani skup, *simplicijalni kompleks na S* je podskup $K(S)$ od $B(S)$ takav da vrijedi

i) $\{s\} \in K(S)$ za svaki $s \in S$ i

ii) ako je $A \subseteq B \subseteq S$ i $B \in K(S)$, tada je $A \in K(S)$.

Ako je $A \in K(S)$, onda A zovemo *stranom* dimenzije $|A| - 1$. Dimenzija simplicijalnog kompleksa je maksimalna dimenzija bilo kojeg elementa kompleksa. Neka je n_i broj strana u $K(S)$ dimenzije i. Primijetimo da je $n_{-1} = 1$ jer je $\emptyset \in K(S)$ te $n_0 = |S|$ zbog svojstva i). *Eulerova karakteristika od $K(S)$* definirana je s

$$\chi(K(S)) = n_0 - n_1 + n_2 - n_3 + \dots.$$

Reducirana Eulerova karakteristika od $K(S)$ definirana je s

$$\chi'(K(S)) = \chi(K(S)) - 1 = -n_{-1} + \chi(K(S)).$$

Ovo se može zapisati i kao

$$\chi'(K(S)) = \sum_{A \in K(S)} (-1)^{\dim(A)}.$$

Neka je X konačan parcijalno uređen skup te $K(X)$ kolekcija svih lanaca u X. Tada je $K(X)$ simplicijalni kompleks kojeg zovemo *kompleksom lanaca od* X. Veza između Eulerove karakteristike kompleksa lanaca od X i Möbiusove funkcije od X dana je u sljedećoj propoziciji.

Propozicija 3.22. *Neka je* X *konačan parcijalno uređen skup s* 0 *i* 1*, skup* $S = X \backslash \{0, 1\}$ *te* $K(S)$ *kompleks lanaca od* S*. Tada vrijedi*

$$\mu(0, 1) = \chi'(K(S)).$$

Dokaz. Svakom lancu C u S možemo pridružiti lanac $C' = C \cup \{0, 1\}$ u X. Svaki lanac u X od 0 do 1 može se dobiti na ovaj način. Tvrdnja sada slijedi iz korolara 3.8. □

Korolar 3.23. *Neka je* X *konačan parcijalano uređen skup s* 0 *i* 1 *te* $K(X)$ *kompleks lanaca od* X*. Tada je* $\chi(K(X)) = 1$*.*

Dokaz. Neka je $x \in X$. Označimo s $S_{0,x}$ kolekciju svih lanaca u X od 0 do x te sa $S_{x,1}$ kolekciju svih lanaca u X od x do 1. Nadalje, neka je T kolekcija svih lanaca u $X \backslash \{0, 1\}$. Tada se kompleks lanaca od X može napisati kao disjunktna unija

$$K(X) = T \cup \left(\bigcup_{x \in X} S_{0,x} \right) \cup \left(\bigcup_{x > 0} S_{x,1} \right).$$

Po propoziciji 3.22 vrijedi

$$\sum_{t \in T} (-1)^{\dim(t)} = \chi(K(X \backslash \{0, 1\})) = \mu(0, 1) + 1,$$

pri čemu suma ide po svim nepraznim $t \in T$. Po korolaru 3.8 za $x \in X$ vrijedi

$$\sum_{s \in S_{0,x}} (-1)^{\dim(s)} = \mu(0, x)$$

i

$$\sum_{s \in S_{x,1}} (-1)^{\dim(s)} = \mu(x, 1).$$

Iz propozicije 3.6 slijedi

$$\sum_{x \in X} \mu(0, x) = 0$$

i

$$\sum_{x > 0} \mu(x, 1) = -\mu(0, 1).$$

Tvrdnja korolara sada slijedi iz

$$\begin{aligned} \chi(K(X)) &= \chi(T) + \chi\left(\bigcup_{x \in X} S_{0,x}\right) + \chi\left(\bigcup_{x > 0} S_{x,1}\right) \\ &= \mu(0,1) + 1 + \sum_{x \in X} \mu(0, x) + \sum_{x > 0} \mu(x, 1) \\ &= \mu(0,1) + 1 + 0 - \mu(0,1) = 1. \end{aligned}$$

□

Navedimo sada primjere u kojima se primjenjuje Möbiusova inverzija. Polje F je komutativni prsten s jedinicom u kojem je svaki nenul element invertibilan. Ako je K polje koje sadrži potpolje F, onda K zovemo *proširenjem* polja F. Izraz oblika

$$f(x) \coloneqq a_0 + a_1 x + \cdots + a_n x^n,$$

gdje su $n \in \mathbb{N}_0$, $a_0, \ldots, a_n \in F, a_n \neq 0$ nazivamo *polinomom n-tog stupnja nad F*. Brojeve $a_0, \ldots, a_n$ zovemo *koeficijentima polinoma*, a_n *vodećim koeficijentom* te a_0 *slobodnim koeficijentom*. Skup svih polinoma nad F označavamo s $F[x]$. Element $\alpha \in F$ nazivamo *nultočkom* polinoma $f \in F[x]$ ako vrijedi $f(\alpha) = 0$. Polinom $f \in F[x]$ je *ireducibilan* ako ne postoje polinomi $g, h \in F[x]$ stupnjeva većih ili jednakih 1 takvi da vrijedi $f = g \cdot h$. *Minimalni polinom* od $\alpha \in F$ je ireducibilni polinom najmanjeg stupnja vodećeg koeficijenta 1 kojem je α nultočka. *Polje cijepanja* polinoma $f \in F[x]$ je najmanje proširenje polja F nad kojim se f može zapisati kao produkt linearnih faktora. Polje K nazivamo *algebarski zatvorenim* ako svaki nekonstantni polinom $f(x) \in K[x]$ ima nultočku u K. *Algebarski zatvarač* polja F je algebarsko proširenje od F koje je algebarski zatvoreno. Ukoliko za polinom $f \in F[x]$ stupnja n vrijedi da ima točno n različitih nultočaka kažemo da je *separabilan*.

Primjer 3.24. *Neka je F konačno polje sa q elemenata. Odredimo $A(n)$, broj ireducibilnih polinoma stupnja n s koeficijentima u F kojima je vodeći koeficijent jednak 1.*

Neka je K proširenje polja F dimenzije n. Tada je K polje cijepanja separabilnog polinoma $f_n(x) = x^{q^n} - x$ jer svaki nenul element od K zadovoljava jednadžbu $x^{q^n-1} - 1 = 0$. Ako je $\alpha \in K$, $\alpha \neq 0$, tada minimalni polinom od α, u oznaci $p_\alpha(x) \in F[x]$, dijeli $f_n(x)$. Označimo s $F[\alpha]$ najmanje potpolje od K koje sadrži F i α. Zbog toga što je $F[\alpha]$ potpolje od K, slijedi da $deg(p_\alpha(x))$ dijeli n. Zbog jedinstvenosti konačnog polja reda q^n u algebarskom zatvaraču od F, bilo koji ireducibilni polinom $q(x) \in F[x]$ čiji stupanj dijeli n mora dijeliti $f_n(x)$. Iz toga slijedi

$$|\{\beta \in K \mid F[\beta] \text{ je dimenzije } d\}| = \begin{cases} d \cdot A(d), & \text{ako } d \mid n, \\ 0, & \text{inače.} \end{cases}$$

Kada elemente od K promatramo u terminima stupnjeva njihovih polinoma nad F dobijemo

$$q^n = \sum_{d|n} d \cdot A(d).$$

S lijeve strane prethodne jednakosti je stupanj produkta svih ireducibilnih polinoma s koeficijentima u F, vodećeg koeficijenta 1, čiji stupanj dijeli n, a s desne strane je suma stupnjeva ireducibilnih faktora istog tog produkta. Koristeći Möbiusovu inverziju dobijemo

$$n \cdot A(n) = \sum_{d|n} \mu(d, n) \cdot q^d,$$

to jest

$$A(n) = \frac{1}{n} \cdot \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot q^d.$$

Iz prethodnog izraza slijedi da je traženi broj $A(n) > 0$ za sve prirodne brojeve n.

Primjer 3.25. *U ovom primjeru računamo izraz za n-ti ciklotomski polinom. Kompleksan broj ζ je **primitivni n-ti korijen jedinice** ako je n najmanji pozitivni cijeli broj takav da je $\zeta^n = 1$. Neka je S skup rješenja jednadžbe $x^n - 1 = 0$. Tada S čini cikličku grupu generiranu bilo koji primitivnim n-tim korijenom jedinice. Svaki $s \in S$ je primitivni k-ti korijen jedinice za neki k koji dijeli n. Polinom*

$$\phi_k(x) = \prod (x - \zeta_i)$$

pri čemu produkt ide po svim primitivnim k-tim korijenima jedinice $\zeta_i \in S$ zove se ***k-ti ciklotomski polinom****. Jasno je da vrijedi*

$$\prod_{\zeta \in S}(x-\zeta) = x^n - 1 = \prod_{k|n} \phi_k(x).$$

Prethodni izraz osigurava da je $\phi_n(x)$ polinom s cjelobrojnim koeficijentima gdje je vodeći koeficijent jednak 1. Pokažimo prethodnu tvrdnju indukcijom po $n \in \mathbb{N}$. Vrijedi $\phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Pretpostavimo da je $n > 1$. Vrijedi

$$x^n - 1 = \prod_{k|n} \phi_k(x) = \phi_n(x) \cdot p(x),$$

pri čemu je $p(x) = \prod_{\substack{k|n \\ k \neq n}} \phi_k(x)$. Po pretpostavci indukcije je $\phi_k(x) \in \mathbb{Z}[x]$ vodećeg koeficijenta 1 za $k \mid n, k \neq n$. Slijedi $p(x) \in \mathbb{Z}[x]$, također vodećeg koeficijenta 1. Iz

$$\phi_n(x) = \frac{x^n - 1}{p(x)}$$

slijedi da je $\phi_n(x) \in \mathbb{Z}[x]$ vodećeg koeficijenta 1. Ako je x dovoljno velik realan broj, onda je $\phi_k(x)$ pozitivan za svaki cijeli broj k koji dijeli n. Tada je moguće izračunati logaritam obje strane te dobiti

$$\ln(x^n - 1) = \sum_{k|n} \ln(\phi_k(x)).$$

Koristeći Möbiusovu inverziju dobijemo

$$\begin{aligned} \ln(\phi_n(x)) &= \sum_{k|n} \mu(k,n) \cdot \ln(x^k - 1) \\ &= \sum_{k|n} \mu\left(\frac{n}{k}\right) \cdot \ln(x^k - 1) \\ &= \ln\left[\prod_{k|n} (x^k - 1)^{\mu\left(\frac{n}{k}\right)}\right]. \end{aligned}$$

Za dovoljno velik realan broj x imamo

$$\phi_n(x) = \prod_{k|n} (x^n - 1)^{\mu\left(\frac{n}{k}\right)}.$$

Desna strana prethodne jednakosti je racionalna funkcija pa možemo pisati

$$\prod_{k|n}(x^k-1)^{\mu\left(\frac{n}{k}\right)}=\frac{a(x)}{b(x)},$$

pri čemu su $a(x)$ i $b(x)$ relativno prosti polinomi s cjelobrojnim koeficijentima. Pretpostavimo da je $b(x)$ polinom stupnja barem 1 te zapišimo

$$\frac{a(x)}{b(x)}=\alpha(x)+\frac{\beta(x)}{b(x)},$$

pri čemu su $\alpha(x)$ i $\beta(x)$ polinomi s cjelobrojnim koeficijentima te $deg(\beta(x)) < deg(b(x))$. Za dovoljno velik pozitivan cijeli broj x imamo $\left|\frac{\beta(x)}{b(x)}\right|<1$ pa stoga vrijedi $\beta(x)=0$ jer su $\phi_n(x)$ i $\alpha(x)$ cjelobrojne vrijednosti. Zaključujemo da je $\prod_{k|n}(x^k-1)^{\mu\left(\frac{n}{k}\right)}$ polinom koji se podudara s $\phi_n(x)$ za beskonačno mnogo vrijednosti x. Time je dokazana jednakost

$$\phi_n(x)=\prod_{k|n}(x^k-1)^{\mu\left(\frac{n}{k}\right)}.$$

Skup svih permutacija skupa $\{1,\dots,n\}$, to jest bijekcija $\sigma\colon\{1,\dots,n\}\to\{1,\dots,n\}$, označavamo s S_n. Uz kompoziciju kao binarnu operaciju, $(S_n,\circ)$ je grupa koju zovemo *simetričnom grupom* stupnja n. *Ciklus* $(i_1i_2\dots i_s)$ je permutacija koja preslikava $i_1\mapsto i_2, i_2\mapsto i_3,\dots,i_s\mapsto i_1$, a ostale elemente iz $\{1,\dots,n\}$ preslikava u same sebe. Broj s nazivamo *duljinom ciklusa*, to jest za prethodni ciklus kažemo da je *s-ciklus*. Za cikluse $\sigma_1=(i_1i_2\dots i_s)$ i $\sigma_2=(j_1j_2\dots j_t)$ kažemo da su *disjunktni* ako je $\{i_1,\dots,i_s\}\cap\{j_1,\dots,j_t\}=\emptyset$. Svaka permutacija može se zapisati kao produkt disjunktnih ciklusa i takav zapis je jedinstven do na poredak ciklusa.

Primjer 3.26. *Neka je S_n simetrična grupa na $\{1,2,\dots,n\}$. Izračunajmo broj permutacija $\sigma\in S_n$ koje nemaju $d_1,d_2,\dots,d_k$-ciklusa kad ih napišemo kao produkt disjunktnih ciklusa.*

Neka je C_i kolekcija ciklusa duljine d_i koji se mogu formirati koristeći elemente iz $\{1,2,\dots,n\}$ te P_i Booleova rešetka skupa C_i, $1\le i\le k$. Promotrimo parcijalno uređen skup $X=P_1\times\dots\times P_k$. Za $A=(A_1,A_2,\dots,A_k)\in X$ neka je $N_=(A)=N_=(A_1,A_2,\dots,A_k)$ oznaka za broj permutacija $\sigma\in S_n$ koje imaju svojstvo da kad se σ zapiše kao produkt disjunktnih ciklusa, d_i-ciklusi od σ su upravo oni ciklusi u A_i za $1\le i\le k$. Slično, s $N_\ge(A)=N_\ge(A_1,A_2,\dots,A_k)$ označimo broj permutacija $\sigma\in S_n$ koje imaju svojstvo

da kad se σ zapiše kao produkt disjunktnih ciklusa, d_i-ciklusi od σ sadrže cikluse iz A_i za $1 \leq i \leq k$. Slijedi

$$N_{\geq}(A) = \sum_{B \geq A} N_{=}(B).$$

Iz propozicije 3.13 znamo da je Möbiusova funkcija od X produkt Möbiusovih funkcija Booleovih rešetki P_i za $1 \leq i \leq k$. Möbiusovu funkciju Boolove rešetke izračunali smo u primjeru 3.15. Posebno, ako je $B = (B_1, B_2, \ldots, B_k)$, onda je

$$\mu((\emptyset, \emptyset, \ldots, \emptyset), (B_1, B_2, \ldots, B_k)) = (-1)^{|B_1|+|B_2|+\cdots+|B_k|}.$$

Ako označimo $\Phi = (\emptyset, \emptyset, \ldots, \emptyset)$ i iskoristimo Möbiusovu inverziju dobijemo

$$N_{=}(\Phi) = \sum_{B \in X} \mu(\Phi, B) \cdot N_{\geq}(B).$$

Jasno je da je $N_{\geq}(B) = 0$ osim ako su svi ciklusi u $\bigcup_{i=1}^{k} B_i$ disjunktni. Ako vrijedi pretpostavka o disjunktnosti i σ sadrži sve cikluse u $\bigcup_{i=1}^{k} B_i$, onda σ može imati bilo koji rastav na cikluse od preostalih $(n - |B_1| \cdot d_1 - \cdots - |B_k| \cdot d_k)$ elemenata. Ako su svi ciklusi u B disjunktni, onda je

$$N_{\geq}(B) = (n - |B_1| \cdot d_1 - \cdots - |B_k| \cdot d_k)! \ .$$

Izračunajmo sada $Z(B)$, broj elemenata od $C = (C_1, C_2, \ldots, C_k) \in X$ za koje vrijedi $|C_i| = |B_i|$ za $1 \leq i \leq k$ i koji imaju sve disjunktne cikluse u $\bigcup_{i=1}^{k} C_i$. Da bi izračunali $Z(B)$ konstruirajmo $|B_1|$ disjkuntnih d_1-ciklusa odabirući $|B_1| \cdot d_1$ elemenata od mogućih n, particionirajmo ih u $|B_1|$ blokova dimenzije d_1 i formirajmo ciklus od svakog bloka. Ovo možemo učiniti na

$$\binom{n}{|B_1| \cdot d_1} \cdot \binom{|B_1| \cdot d_1}{d_1, d_1, \ldots, d_1} \cdot \frac{1}{|B_1|!} \cdot ((d_1 - 1)!)^{|B_1|}$$

načina. Od preostalih $n - |B_1| \cdot d_1$ elemenata biramo $|B_2|$ ciklusa duljine d_2. Ovo možemo učiniti na

$$\binom{n - |B_1| \cdot d_1}{|B_2| \cdot d_2} \cdot \binom{|B_2| \cdot d_2}{d_2, d_2, \ldots, d_2} \cdot \frac{1}{|B_2|!} \cdot ((d_2 - 1)!)^{|B_2|}$$

načina. Nastavljamo ovaj postupak dok nisu odabrani svi $d_1, d_1, \ldots, d_k$-ciklusi. Nakon pojednostavljivanja produkta svih izraza dobijemo

$$Z(B) = \frac{n!}{(d_1)^{|B_1|} \cdot |B_1|! \ldots (d_k)^{|B_k|} \cdot |B_k|!}.$$

Zbog toga vrijedi

$$\begin{aligned} N_{=}(\emptyset, \emptyset, \ldots, \emptyset) &= n! \cdot \sum \frac{(-1)^{n_1 + \cdots + n_k}}{(d_1)^{n_1} \cdot n_1! \ldots (d_k)^{n_k} \cdot n_k!} \\ &= n! \cdot \sum \left(\prod_{i=1}^{k} \frac{(-1)^{n_i}}{(d_i)^{n_i} \cdot n_i!} \right), \end{aligned}$$

pri čemu suma ide po svim k-torkama nenegativnih cijelih brojeva $(n_1, \ldots, n_k)$ takvim da je $n_1 \cdot d_1 + \cdots + n_k \cdot d_k \leq n$. S obzirom na to da vrijedi

$$e^{\frac{-1}{d_i}} = \sum_{n=0}^{\infty} \frac{(-1)^n}{(d_i)^n \cdot n!},$$

zaključujemo da je vjerojatnost slučajno odabrane permutacije iz S_n napisane kao produkt disjunktnih ciklusa koja ne sadrži cikluse duljine $d_1, d_2, \ldots, d_k$ teži k

$$e^{\frac{-1}{d_1}} \ldots e^{\frac{-1}{d_k}}$$

kad n teži u beskonačnost.

4 Podalgebre

Neka su A i B prsteni. Kažemo da je A *izomorfan potprstenu* od B ako postoji injektivni homomorfizam $\phi\colon A \to B$. Dodatno, ako su A i B prsteni s jedinicama i vrijedi $\phi(1_A) = 1_B$, kažemo da je A *uložen* u B. Slično, ako su A i B asocijativne R-algebre s jedinicama kažemo da je A *izomorfna podalgebri* od B i A *uložena* u B.

Propozicija 4.1. *Neka je R komutativni prsten s jedinicom. Ako je X' podskup parcijalno uređenog skupa X, onda je $I(X', R)$ podalgebra od $I(X, R)$.*

Podalgebra $I(X', R)$ sastoji se od funkcija $f \in I(X, R)$ takvih da vrijedi $f(x, y) = 0$ ako $x \notin X'$ ili $y \notin X'$.

Definicija 4.2. *Neka je R prsten. Podskup $S \subseteq R$ je **lijevi** (tj. **desni**) **ideal** u R ako vrijedi*

i) S je potprsten od R i

ii) za sve $r \in R$ i $s \in S$ vrijedi $rs \in S$ (tj. $sr \in S$).

*Podskup $S \subseteq R$ je (dvostrani) **ideal** ako je istovremeno lijevi i desni ideal.*

Propozicija 4.3. *Neka je X parcijalno uređen skup, R komutativni prsten s jedinicom te $S \subseteq R$ ideal od R. Tada je $I(X, S)$ podalgebra od $I(X, R)$.*

Podalgebra $I(X, S)$ sastoji se od funkcija $f \in I(X, R)$ takvih da vrijedi $f(x, y) \in S$ za sve $x, y \in X$. Predstavimo sada klasu podalgebri koje su nam od većeg interesa od prethodno navedenih. Prisjetimo se najprije pojma klase ekvivalencije. Neka je $\sim$ relacija ekvivalencije na nepraznom skupu A, te neka je $a \in A$. Skup

$$[a] \coloneqq \{x \in A \mid a \sim x\}$$

zovemo *klasom ekvivalencije* elementa a. Skup svih klasa ekvivalencije zovemo *kvocijentnim skupom* i označavamo ga s $A/_\sim$.

Definicija 4.4. *Neka je E relacija ekvivalencije na skupu nepraznih intervala od X. Funkcija $f \in I(X, R)$ je **E-funkcija** ako $[x, y]E[u, v]$ povlači $f(x, y) = f(u, v)$, to jest ako je f konstanta na klasama ekvivalencije od E.*

Kolekciju E-funkcija u $I(X, R)$ označavat ćemo s $I(X_E, R)$.

Definicija 4.5. *Neka je E relacija ekvivalencije na skupu nepraznih intervala od X.*

i) E nazivamo ***redno kompatibilnom*** *ako je $f * g$ E-funkcija kadgod su f i g E-funkcije. Klase ekvivalencije od E nazivamo* ***tipovima****.*

ii) E nazivamo ***relacijom S-ekvivalencije*** *ako kadgod je $[x, y]E[u, v]$, tada postoji bijektivno preslikavanje $\varphi\colon [x, y] \to [u, v]$ takvo da za sve $z \in [x, y]$ vrijedi $[x, z]E[u, \varphi(z)]$ i $[z, y]E[\varphi(z), v]$.*

Primijetimo da je $I(X_E, R)$ podalgebra od $I(X, R)$ ako i samo ako je E redno kompatibilna. Dodatno, jasno je da je izomorfizam relacija S-ekvivalencije. Pokazat ćemo da su relacije S-ekvivalencije usko povezane s redno kompatibilnim relacijama ekvivalencije.

Neka je R prsten. Pretpostavimo da postoji $m \in \mathbb{N}$ takav da vrijedi

$$mx = 0, \quad \forall x \in R.$$

Karakteristika prstena R je minimalan takav m koji zadovoljava prethodnu jednakost. Ukoliko takav m ne postoji, kažemo da je prsten R *karakteristike nula.*

Propozicija 4.6. *Neka je X lokalno konačan parcijalno uređen skup, R komutativni prsten s jedinicom te E relacija ekvivalencije na skupu nepraznih intervala od X.*

(a) Ako je E relacija S-ekvivalencije, onda je $I(X_E, R)$ podalgebra od $I(X, R)$.

(b) Ako je $I(X_E, R)$ podalgebra od $I(X, R)$ i R je prsten karakteristike 0, onda je E relacija S-ekvivalencije.

Dokaz. (a) S obzirom da je E relacija S-ekvivalencije, kadgod je $[x, y]E[u, v]$, tada postoji bijektivno preslikavanje

$$\varphi\colon [x, y] \to [u, v]$$

takvo da za sve $z \in [x, y]$ vrijedi $[x, z]E[u, \varphi(z)]$ i $[z, y]E[\varphi(z), v]$. Za dane $f, g \in I(X_E, R)$ vrijedi

$$\begin{aligned}(f * g)(x, y) &= \sum_{x \le z \le y} f(x, z) \cdot g(z, y) \\ &= \sum_{x \le z \le y} f(u, \varphi(z)) \cdot g(\varphi(z), v) \\ &= \sum_{u \le t \le v} f(u, t) \cdot g(t, v) \\ &= (f * g)(u, v).\end{aligned}$$

Iz prethodnog računa slijedi da je E redno kompatibilna, odnosno da je $I(X_E, R)$ podalgebra od $I(X, R)$.

(b) Pretpostavimo da je $I(X_E, R)$ podalgebra od $I(X, R)$, R karakteristike nula te $[x, y]E[u, v]$ za neke $[x, y], [u, v] \subseteq X$. Neka je E' relacija ekvivalencije na $[x, y]$ definirana s $sE't$ ako $[x, s]E[x, t]$ i $[s, y]E[t, y]$ za $s, t \in [x, y]$. Označimo s P' particiju koja se sastoji od klasa ekvivalencije od E' na $[x, y]$. Analogno definiramo relaciju ekvivalencije E'' na $[u, v]$ i označimo s P'' particiju koju ona određuje na $[u, v]$. Za $\xi \in P'$ definiramo

$$\Psi(\xi) = \{t \in [u, v] \mid [x, s]E[u, t] \text{ i } [s, y]E[t, v] \text{ za neki } s \in \xi\}.$$

Pokažimo da skupovi $\Psi(\xi)$ i ξ imaju jednak broj elemenata. Neka je f E-funkcija definirana s

$$f(a, b) = \begin{cases} 1, & \text{ako je } [a, b]E[x, s] \text{ za neki } s \in \xi, \\ 0, & \text{inače,} \end{cases}$$

te neka je g E-funkcija definirana s

$$g(c, d) = \begin{cases} 1, & \text{ako je } [c, d]E[s, y] \text{ za neki } s \in \xi, \\ 0, & \text{inače.} \end{cases}$$

$I(X_E, R)$ je podalgebra pa vrijedi $f*g \in I(X_E, R)$ i $(f*g)(x, y) = (f*g)(u, v)$. Iz

$$f(x, s) \cdot g(s, y) = \begin{cases} 1, & \text{ako je } s \in \xi, \\ 0, & \text{inače,} \end{cases}$$

slijedi

$$(f * g)(x, y) = \sum_{x \leq s \leq y} f(x, s) \cdot g(s, y) = |\xi| \cdot 1.$$

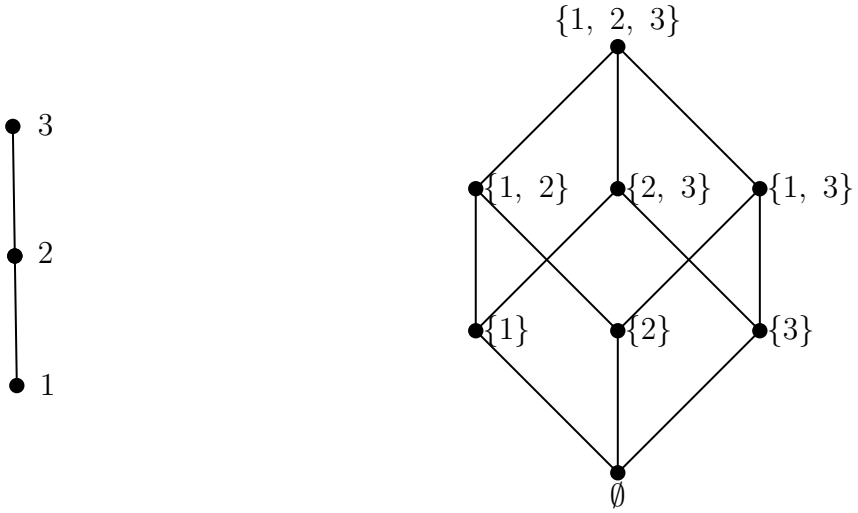
Sličnim argumentiranjem pokaže se i

$$(f * g)(u, v) = |\Psi(\xi)| \cdot 1.$$

S obzirom da je R prsten karakteristike nula, slijedi tvrdnja $|\Psi(\xi)| = |\xi|$. Lako se vidi da vrijedi $\Psi(\xi) \in P''$ pa je $\Psi \colon P' \to P''$ bijekcija koja zadovoljava svojstvo da ako su $s \in \xi$ te $t \in \Psi(\xi)$, onda $[x, s]E[u, t]$ i $[s, y]E[t, v]$. Konačno, neka je $\varphi \colon [x, y] \to [u, v]$ bilo koja bijekcija koja zadovoljava $\{\varphi(s) \mid s \in \xi\} = \Psi(\xi)$ za sve $\xi \in P'$. Tada je φ traženo preslikavanje iz definicije relacije S-ekvivalencije E. □

Napomenimo da su intervali parcijalno uređenog skupa izomorfni ako su izomorfni kao parcijalno uređeni skupovi, to jest $[x, y] \simeq [u, v]$ ako postoji bijekcija $\varphi\colon [x, y] \to [u, v]$ takva da za sve $s, t \in [x, y]$ vrijedi nejednakost $\varphi(s) \leq \varphi(t)$ ako i samo ako je $s \leq t$. Sljedeći primjer ilustrira ovu vrstu podalgebre.

Konačan parcijalno uređeni skup $(X, \leq)$ možemo prikazati takozvanim *Hasseovim dijagramom*. Riječ je o usmjerenom grafu sa skupom vrhova X i lukovima (usmjerenim bridovima) (x, y) kadgod vrijedi $x < y$ te ne postoji $z \in X$ takav da vrijedi $x < z < y$. Hasseov dijagram prikazujemo tako da su „manji " vrhovi ispod „većih", to jest lukovi su usmjereni odozdo prema gore. Na primjer, Hasseov dijagram skupa $N = \{1, 2, 3\}$ s prirodnim totalnim uređajem prikazan je slici 4.1 lijevo. Hasseov dijagram Booleve rešetke B_3 prikazan je na slici 4.1 desno.



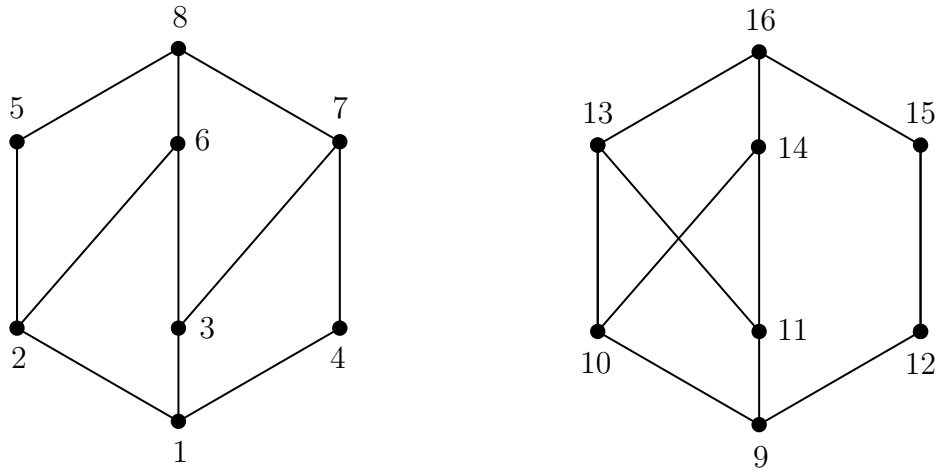
Slika 4.1: Hasseovi dijagrami od $(\{1, 2, 3\}, \leq)$ i $(B_3, \subseteq)$.

Primjer 4.7. *Neka je $X = \{1, 2, \ldots, 16\}$ parcijalno uređen skup čiji je Hasseov dijagram prikazan na slici 4.2 ispod te neka je F polje.*

Definirajmo relaciju ekvivalencije E na nepraznim intervalima od X na sljedeći način. Dva intervala u X su u relaciji E ako su izomorfni ili ako su ta dva intervala intervali $[1, 8]$ i $[9, 16]$. Lako se vidi da je E zaista relacija ekvivalencije. Ako su $[x, y]$ i $[u, v]$ izomorfni, onda je očiti izbor za preliskavanje φ iz definicije S-ekvivalentne relacije 4.5. Za intervale $[1, 8]$ i $[9, 16]$ uzmimo preslikavanje dano s

$$z \to z + 8.$$

Iz propozicije 4.6 slijedi da je $I(X_E, F)$ podalgebra od $I(X, F)$.



Slika 4.2: Hasseov dijagram parcijalno uređenog skupa $X = \{1, 2, \ldots, 16\}$.

Relaciju E na skupu nepraznih intervala parcijalno uređenog skupa $(X, \leq)$ za koju vrijedi $[x, y]E[u, v]$ ako i samo ako su $[x, y]$ i $[u, v]$ izomorfni kao parcijalno uređeni skupovi nazivamo *izomorfizmom.*

Definicija 4.8. *Ako je E redno kompatibilna relacija ekvivalencije na skupu nepraznih intervala parcijalno uređenog skupa X te R komutativni prsten s jedinicom, tada podalgebru $I(X_E, R)$ nazivamo* ***reduciranom indicencijskom algebrom od X nad*** *R i označavamo s $\mathrm{Red}_E(I(X, R))$ ili jednostavnije $\mathrm{Red}(I(X, R))$. Ako je E izomorfizam, onda podalgebru nazivamo* ***standardnom reduciranom incidencijskom algebrom od X nad*** *R.*

U sljedećoj propoziciji opisat ćemo reducirane incidencijske podalgebre incidencijskih algebri konačnih parcijalno uređenih skupova nad poljem.

Za $f, g \in I(X, R)$ definiramo *Hadamardov produkt od f i g*, u oznaci $f \odot g$, s $(f \odot g)(x, y) = f(x, y) \cdot g(x, y)$ za sve $x, y \in X$. Jasno je da je $f \odot g \in I(X, R)$ za $f, g \in I(X, R)$ te da je produkt komutativan. Hadamardov produkt ponekad se naziva i *Schurovim produktom.*

Propozicija 4.9. *Neka je X konačan parcijalno uređen skup te F polje. Podalgebra A od $I(X, F)$ je reducirana incidencijska podalgebra ako i samo ako vrijedi*

(a) $\zeta \in A$ i

(b) ako je $f, g \in A$, onda je $f \odot g \in A$.

Dokaz. Kada je A reducirana incidencijska podalgebra s obzirom na relaciju ekvivalencije E, funkcija ζ je sadržana u A. Naime, za $[x_1, y_1]E[x_2, y_2]$ zbog

tranzitivnosti parcijalnog uređaja vrijedi $x_1 \leq y_1$ i $x_2 \leq y_2$ pa je $\zeta(x_1, y_1) = \zeta(x_2, y_2) = 1$, to jest ζ je E-funkcija. Nadalje, za $f, g \in A$ vrijedi $f(x_1, y_1) = f(x_2, y_2)$ i $g(x_1, y_1) = g(x_2, y_2)$. Slijedi

$$\begin{aligned}(f \odot g)(x_1, y_1) &= f(x_1, y_1) \cdot g(x_1, y_2) \\ &= f(x_2, y_2) \cdot g(x_2, y_2) \\ &= (f \odot g)(x_2, y_2).\end{aligned}$$

Ovime smo pokazali da je A zatvorena s obzirom na Hadamardov produkt.

Obrnuto, definirajmo relaciju E na intervalima od X s $[x_1, y_1]E[x_2, y_2]$ ako $f(x_1, y_1) = f(x_2, y_2)$ za sve $f \in A$. Lako se vidi da je E relacija ekivalencije. Označimo s $\alpha_1, \alpha_2, \ldots, \alpha_n$ različite klase ekvivalencije relacije E. Ako je $i \neq j$, onda postoji $f_{ij} \in A$ takva da vrijedi $f_{ij}(\alpha_i) \neq f_{ij}(\alpha_j)$. Definirajmo funkcije ϕ_{ij} s

$$\phi_{ij} = \frac{f_{ij} - f_{ij}(\alpha_j) \cdot \zeta}{f_{ij}(\alpha_i) - f_{ij}(\alpha_j)}.$$

Tada vrijedi $\phi_{ij}(\alpha_i) = 1$ i $\phi_{ij}(\alpha_j) = 0$. Po pretpostavci Hadamardov produkt

$$\Phi_i = \prod_{j \neq i} \phi_{ij}$$

je u A. S obzirom da vrijedi $\Phi_i(\alpha_i) = 1$ i $\Phi_i(\alpha_j) = 0$ za $i \neq j$, skup $\{\Phi_1, \Phi_2, \ldots, \Phi_n\}$ čini bazu za podalgebru od $I(X, F)$ koja sadrži funkcije koje su konstantne na klasama ekvivalencije od E. Dakle, A je skup svih takvih funkcija. S obzirom da je A zatvorena s obzirom na množenje u $I(X, F)$, A je reducirana incidencijska podalgebra. □

Prirodni primjer reducirane incidencijske podalgebre je standardna reducirana incidencijska algebra. Reducirane incidencijske algebre se proučavaju od 1960-ih. Pokazat ćemo dva primjera koja će nam ilustrirati korisnost takvih podalgebri.

Primjer 4.10. *Neka je $I(\mathbb{N}_0, R)$ incidencijska algebra pri čemu je R komutativni prsten s jedinicom te $\mathbb{N}_0$ skup svih prirodnih brojeva s nulom.*

S obzirom da vrijedi $[x, y] \simeq [u, v]$ ako i samo ako $y - x = v - u$, ako je f u standardnoj reduciranoj incidencijskoj algebri, tada je f određena vrijednostima od $f(0, n)$ za sve $n \in \mathbb{N}_0$. Neka je $a_n = f(0, n)$ te bijekcija

$$f \longmapsto a_0 + a_1 t + a_2 t^2 + \ldots$$

koja funkciji f pridružuje red potencija s varijablom t. Tada imamo preslikavanje

$$\rho \colon \mathrm{Red}_{\simeq}(I(X, R)) \longmapsto R[[t]],$$

pri čemu je $R[[t]]$ prsten formalnih redova potencija s koeficijentima u R. Preslikavanje ρ je preslikavanje R-modula. Ako je

$$g \longmapsto b_0 + b_1 t + b_2 t^2 + \dots,$$

onda je

$$\begin{aligned}(f * g)(0,n) &= \sum_{i=0}^{n} f(0,i) \cdot g(i,n) \\ &= \sum_{i=0}^{n} f(0,i) \cdot g(0,n-i) \\ &= \sum_{i=0}^{n} a_i \cdot b_{n-i}.\end{aligned}$$

Množenje u $\mathrm{Red}_{\simeq}(I(\mathbb{N}_0, R))$ odgovara množenju redova potencija. Slijedi izomorfizam R-algebri $\mathrm{Red}_{\simeq}(I(\mathbb{N}_0, R)) \simeq R[[t]]$. Posebno, iz

$$\zeta \longmapsto 1 + t + t^2 + \dots = \frac{1}{1-t}$$

slijedi $\zeta^{-1} = \mu = 1 - t$. Stoga vrijedi

$$\mu(x,y) = \begin{cases} 1, & \text{ako je } x = y, \\ -1, & \text{ako je } y = x+1, \\ 0, & \text{inače.} \end{cases}$$

Primjer 4.11. *Neka je $\mathbb{N}$ skup svih prirodnih brojeva parcijalno uređenih relacijom djeljivost, R komutativni prsten s jedinicom te neka je*

$$A = \left\{ f \in I(\mathbb{N}, R) \mid f(x_1, y_1) = f(x_2, y_2) \text{ ako } \frac{y_1}{x_1} = \frac{y_2}{x_2} \right\}.$$

Podalgebra A je reducirana incidencijska podalgebra koja sadrži standardnu reduciranu incidencijsku algebru. Za $f \in A$ imamo jednakost $f(x,y) = f(1, \frac{y}{x})$ pa je f određena vrijednostima $f(1,n)$ za sve prirodne brojeve n. Funkcija $f \in A$ je u $\mathrm{Red}_{\simeq}(I(\mathbb{N}, R))$ ako vrijedi $f(x_1, y_1) = f(x_2, y_2)$ kadgod je familija eksponenata u rastavu broja $\frac{y_1}{x_1}$ na proste faktore jednaka familiji eksponenata of $\frac{y_2}{x_2}$.

U slučaju kad je R polje kompleksnih brojeva $\mathbb{C}$ postoji poznata reprezentacija reduciranih incidencijskih algebri. Neka je $a_n = f(1,n)$. Promotrimo bijekciju

$$f \longmapsto \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

pri čemu je s fiksan kompleksan broj. Takav red naziva se Dirichletovim redom. Ako je

$$g \longmapsto \sum_{n=1}^{\infty} \frac{b_n}{n^s},$$

onda vrijedi

$$\begin{aligned}(f * g)(1,n) &= \sum_{r|n} f(1,r) \cdot g(r,n) \\ &= \sum_{r|n} f(1,r) \cdot g\left(1, \frac{n}{r}\right) \\ &= \sum_{r|n} a_n \cdot b_{\frac{n}{r}}.\end{aligned}$$

Ako je

$$\left(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right) \cdot \left(\sum_{n=1}^{\infty} \frac{b_n}{n^s}\right) = \left(\sum_{n=1}^{\infty} \frac{c_n}{n^s}\right),$$

onda je

$$\frac{c_n}{n^s} = \sum_{r|n} \frac{a_r}{r^s} \cdot \frac{b_{(\frac{n}{r})}}{(\frac{n}{r})^s} = \sum_{r|n} \frac{a_n \cdot b_{\frac{n}{r}}}{n^s},$$

što povlači

$$c_n = \sum_{r|n} a_n \cdot b_{\frac{n}{r}}.$$

Ovime smo pokazali da množenje odgovara množenju Dirichletovih redova pa slijedi da je standardna reducirana incidencijska algebra $\mathrm{Red}_{\simeq}(I(\mathbb{N}, \mathbb{C}))$ *izomorfna podalgebri algebre Dirichletovih redova. Specijalno,*

$$\zeta \longmapsto \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s),$$

je klasična Riemannova zeta funkcija. Prema tome vrijedi

$$\mu \longmapsto \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

gdje je μ inverz od ζ u incidencijskoj algebri $I(\mathbb{N}, \mathbb{C})$ te $\mu(n)$ klasična Möbiusova funkcija iz trećeg poglavlja.

Literatura

[1] Z.Bujanović, B.Muha, *Elementarna matematika* 1, skripta, Sveučilište u Zagrebu, 2018.
`https://web.math.pmf.unizg.hr/nastava/em/em1/materijali/EM1-skripta.pdf` (prosinac 2022.)

[2] V.Krčadinac, *Kombinatorika*, skripta, Sveučilište u Zagrebu, 2022.
`https://web.math.pmf.unizg.hr/~krcko/nastava/komb/komb-skripta.pdf` (studeni 2022.)

[3] A.Paulin, *Introduction to Abstract Algebra*, University of California, Berkeley, 2018.
`https://math.berkeley.edu/~apaulin/AbstractAlgebra.pdf` (kolovoz 2022.)

[4] G.-C. Rota, *On the foundations of combinatorial theory. I. Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete 2 (1964), 340–368.

[5] J. J. Rotman, *Advanced modern algebra*, American Mathematical Society, Providence, Rhode Island, 2015.

[6] E. Spiegel, C. J. O'Donnell, *Incidence algebras*, Marcel Dekker, Inc., 1997.

[7] B.Širola, *Algebarske strukture*, skripta, Sveučilište u Zagrebu, 2010.
`https://web.math.pmf.unizg.hr/nastava/alg_prof/predavanja/ASpred.pdf` (kolovoz 2022.)

[8] M.Vuković, *Teorija skupova*, skripta, Sveučilište u Zagrebu, 2015.
`https://web.math.pmf.unizg.hr/nastava/ts/materijali/ts-skripta-2015.pdf` (srpanj 2022.)

Sažetak

U ovom radu proučavali smo incidencijske algebre. Na početku smo definirali parcijalno uređen skup, lokalnu konačnost parcijalno uređenog skupa te naveli nekoliko primjera. Nakon toga uveden je pojam incidencijske algebre lokalno konačnog parcijalno uređenog skupa nad komutativnim prstenom R s jedinicom. Pokazano je da je incidencijska algebra po strukturi asocijativna R-algebra s jedinicom te da se može uložiti u algebru trokutastih matrica. Središnji dio rada bavi se računanjem Möbiusove funkcije na elementima parcijalno uređenog skupa te generaliziranim formulama Möbiusove inverzije. Primjena Möbiusove inverzije ilustrirana je na primjerima iz kombinatorike. Nadalje, definirali smo pojam E-funkcije incidencijske algebre, gdje je E relacija ekvivalencije te je pokazana veza između incidencijske algebre i skupa svih E-funkcija u njoj. Uveden je pojam reducirane incidencijske algebre te je dana karakterizacija reducirane incidencijske podalgebre konačnog parcijalno uređenog skupa nad poljem. Konačno, dani su primjeri koji nam pokazuju vezu reduciranih incidencijskih podalgebri s prstenima formalnih redova potencija.

Summary

In this thesis we study incidence algebras. At the beginning, we define a partially ordered set, local finiteness of a partially ordered set and give several examples. After that we introduce the concept of incidence algebra of a locally finite partially ordered set over a commutative ring R with identity. It is shown that the incidence algebra is an associative R-algebra with identity and that it can be embedded into the algebra of triangular matrices. The central part of the thesis deals with the calculation of the Möbius function on the elements of a partially ordered set and with the generalized formulas of Möbius inversion. Applications of Möbius inversion are illustrated by examples from combinatorics. In addition, we define the concept of E-functions in an incidence algebra, where E is an equivalence relation, and we show the connection between the incidence algebra and the set of all E-functions in it. The concept of reduced incidence algebra is introduced and a characterization of the reduced incidence subalgebra of a finite partially ordered set over a field is given. Finally, we give examples that show connections between reduced incidence subalgebras and rings of formal power series.

Životopis

Rodena sam 6. rujna 1998. godine u Gospiću. Osnovnu školu sam pohađala u Ličkom Lešću, a nakon toga srednju školu u Otočcu, smjer opća gimnazija. Nakon završene srednje škole, 2017. godine upisujem preddiplomski studij Matematika na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Godine 2020. završavam preddiplomski studij te iste godine upisujem diplomski sveučilišni studij Financijska i poslovna matematika na istom fakultetu.