Elementarna matematika
- predavanja -

November 10, 2015

Sadržaj

Deo I

Zasnivanje prirodnih, celih, racionalnih, realnih i kompleksnih brojeva

I.1 Peanove aksiome

Definicija 1 Za uređenu trojku $(P, \mathbf{1}, f)$ kažemo da je *struktura prirodnih brojeva* ako je $\mathbf{1} \in P$, f je funkcija pri čemu $f : P \to P$ i važi:

(P1) $\forall x \in P\ (\mathbf{1} \neq f(x))$

(P2) $\forall x, y \in P(x \neq y \Rightarrow f(x) \neq f(y))$

(P3) ako je $M \subseteq P$ tako da $\mathbf{1} \in M$ i $\forall x \in P(x \in M \Rightarrow f(x) \in M)$ onda je $M = P$.

Za elemente skupa P kažemo da su *prirodni brojevi* te strukture. Za $f(x)$ kažemo da je *sledbenik* broja x. □

Konvencija Umesto $f(x)$ pisaćemo kraće x'. □

U skladu sa prethodnom konvencijom osobine (P1)–(P3) se mogu zapisati na sledeći način:

(P1) $\forall x \in P\ (\mathbf{1} \neq x')$

(P2) $\forall x, y \in P(x \neq y \Rightarrow x' \neq y')$

(P3) ako je $M \subseteq P$ tako da $\mathbf{1} \in M$ i $\forall x \in P(x \in M \Rightarrow x' \in M)$ onda je $M = P$.

Stav 1 $\forall x \in P(x \neq x')$.

Dokaz. Pretpostavimo, suprotno tvrđenju stava, da postoji neko $q \in P$ tako da $q = q'$. Neka $M := P \setminus \{q\}$.

- Na osnovu (P1) ne može biti $\mathbf{1} = \mathbf{1}'$ pa je $\mathbf{1} \in M$.
- Neka $x \in M$. Pokazujemo $x' \in M$. Ako bi bilo $x' \in P \setminus M = \{q\}$ onda $x' = q = q'$ pa, na osnovu (P2), $x = q$, tj. $x \notin M$, kontradikcija.
Dakle na osnovu prethodnog i (P3) imamo da je $M = P$. S druge strane $q \in P \setminus M$, što je nemoguće. □

Stav 2 $x \in P \setminus \{\mathbf{1}\} \Rightarrow \exists y \in P(x = y')$.

Dokaz. Pretpostavimo, suprotno tvrđenju stava, da postoji neko $q \in P \setminus \{\mathbf{1}\}$ tako da $\forall x \in P\ (q \neq x')$. Neka $M := P \setminus \{q\}$.
- Kako $q \neq \mathbf{1}$ to $\mathbf{1} \in M$.
- Neka $x \in M$. Ne može biti $x' = q$ zbog izbora prirodnog broja q. Zato je $x' \in M$.
Na osnovu (P3) je $M = P$, tj. $q \in P = M$ i $q \notin M$, protivurečnost. □

Teorema 1 (*o rekurziji*) Neka su dati struktura prirodnih brojeva $(P, \mathbf{1}, ')$, skup S, preslikavanje $T : P \times S \to S$ i $a_0 \in S$.

Tada postoji jedinstveno preslikavanje $k : P \to S$ tako da važi:
- $k(\mathbf{1}) = a_0$;
- $k(x') = T(x', k(x))$, za svako $x \in P$. □

Teorema o rekurziji dozvoljava definisanje dveju osnovnih operacija u strukturi prirodnih brojeva na sledeći način.

Definicija 2 (*Sabiranje prirodnih brojeva*) Neka je $(P, \mathbf{1}, ')$ s.p.b. i neka je $x \in P$ fiksirano. Posmatrajmo $T : P \times P \to P$ definisano sa $T((y, z)) := z'$. Na osnovu teoreme o rekurziji postoji prelikavanje $\sigma_x : P \to P$ tako da je

(i) $\sigma_x(\mathbf{1}) = x'$,

(ii) $\sigma_x(y') = (\sigma_x(y))'$ za svako $y \in P$.

Na taj način je **za svako** $x \in P$ definisano **po** jedno preslikavanje $\sigma_x : P \to P$ tako da važe uslovi (i) i (ii). Ako su $x, y \in P$ proizvoljni definišimo

$$x + y := \sigma_x(y).$$

Sada se koristeći ovu novu notaciju uslovi (i) i (ii) mogu zapisati i ovako:

(S1) $x + 1 = x'$,

(S2) $x + y' = (x + y)'$

odakle se jasnije vidi način na koji operacija "+" funkcioniše. □

Definicija 3 (*Množenje prirodnih brojeva*) Neka je $(P, \mathbf{1}, ')$ s.p.b. i neka je $x \in P$ fiksirano. Posmatrajmo $T : P \times P \to P$ definisano sa $T((y, z)) := z + x$. Na osnovu teoreme o rekurziji postoji preslikavanje $\delta_x : P \to P$ tako da je

(i) $\delta_x(\mathbf{1}) = x$,

(ii) $\delta_x(y') = \delta_x(y) + x$ za svako $y \in P$.

Ako su $x, y \in P$ proizvoljni definišimo

$$x \cdot y := \delta_x(y).$$

Uslovi (i) i (ii) poprimaju sledeći oblik:
(M1) $x \cdot \mathbf{1} = x$,
(M2) $x \cdot y' = (x \cdot y) + x$. $\square$

Stav 3 Za ovako uvedene operacije "+" i "$\cdot$" važi sledeći zakoni:
1) $x + (y + z) = (x + y) + z$
2) $x + y = y + x$
3) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
4) $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$
5) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
6) $x \cdot \mathbf{1} = \mathbf{1} \cdot x = x$
7) $x \cdot y = y \cdot x$

Dokaz.
1) Pokazujemo $\forall x, y \in P\ (x + (y + z) = (x + y) + z)$ indukcijom po z. Ovo zapravo znači da za skup $M := \{z \in P \mid \forall x, y \in P\ (x + (y + z) = (x + y) + z)\}$ pokazujemo da važi $\mathbf{1} \in M$ i $\forall z\ (z \in M \Rightarrow z' \in M)$.

– $\mathbf{1} \in M$:
Za $z = \mathbf{1}$ imamo $x + (y + \mathbf{1}) =$ (S1): $x + y' =$ (S2): $(x + y)' =$ (S1): $(x + y) + \mathbf{1}$.

– $\forall z\ (z \in M \Rightarrow z' \in M)$:
Neka za dato z važi $x + (y + z) = (x + y) + z$ za svako x, y. Imamo $x + (y + z') =$ (S2): $x + (y + z)' =$ (S2): $(x + (y + z))' =$ I.H.: $((x + y) + z)' =$ (S2): $(x + y) + z'$.

2) Pokazujemo $\forall x\ (x + y = y + x)$ indukcijom po y.
• $y = \mathbf{1}$: Pokazujemo $\forall x\ (x + \mathbf{1} = \mathbf{1} + x)$ indukcijom po x.
Za $x = \mathbf{1}$ imamo $\mathbf{1} + \mathbf{1} = \mathbf{1} + \mathbf{1}$. Neka sada za dato x važi $x + \mathbf{1} = \mathbf{1} + x$. Imamo $x' + \mathbf{1} =$ (S1): $(x + \mathbf{1}) + \mathbf{1} =$ I.H.: $(\mathbf{1} + x) + \mathbf{1} = 1$): $\mathbf{1} + (x + \mathbf{1}) =$ (S1): $\mathbf{1} + x'$. •
Neka sada za dato y važi $\forall x\ (x + y = y + x)$. $x + y' = x + (y + \mathbf{1}) = (x + y) + \mathbf{1} = (y + x) + \mathbf{1} = y + (x + \mathbf{1}) = y + (\mathbf{1} + x) = (y + \mathbf{1}) + x = y' + x$, gde smo koristili (S1), I.H., 1) i 2).
3) Indukcijom po z.
Za $z = \mathbf{1}$ imamo $x \cdot (y + \mathbf{1}) = x \cdot y' = (x \cdot y) + x = (x \cdot y) + (x \cdot \mathbf{1})$, gde smo koristili (S1), (M2) i (M1).
Neka sada važi $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ za svako x, y. Imamo $x \cdot (y + z') = x \cdot (y + z)' = (x \cdot (y + z)) + x = ((x \cdot y) + (x \cdot z)) + x = (x \cdot y) + ((x \cdot z) + x) = (x \cdot y) + (x \cdot z')$, gde smo koristili (S2), (M2), I.H. i 1).
4) Indukcijom po z.

Za $z = \mathbf{1}$ imamo $(x + y) \cdot \mathbf{1} = x + y = (x \cdot \mathbf{1}) + (y \cdot \mathbf{1})$, gde je korišćeno (M1).

Neka sada važi $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ za svako x, y. Imamo $(x + y) \cdot z' = ((x+y)\cdot z)+(x+y) = ((x\cdot z)+(y\cdot z))+(x+y) = ((x\cdot z)+x)+((y\cdot z)+y) = (x\cdot z')+(y\cdot z')$, gde je korišćeno (M2), I.H., 1) i 2).

5) Indukcijom po z.

Za $z = \mathbf{1}$ imamo $x \cdot (y \cdot \mathbf{1}) = x \cdot y = (x \cdot y) \cdot \mathbf{1}$, gde je korišćeno (M1). Neka sada važi $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ za svako x, y. Imamo $x \cdot (y \cdot z') = x \cdot ((y \cdot z) + y) = (x \cdot (y \cdot z)) + (x \cdot y) = ((x \cdot y) \cdot z) + (x \cdot y) = (x \cdot y) \cdot z'$, gde smo koristili (M2), 3) i I.H.

6) Dokazujemo $\forall x\ (\mathbf{1} \cdot x = x)$ indukcijom po x.

Za $x = \mathbf{1}$ imamo $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$ zbog (M1). Neka sada za dato x važi $\mathbf{1} \cdot x = x$. Imamo $\mathbf{1} \cdot x' = (\mathbf{1} \cdot x) + \mathbf{1} = x + 1 = x'$, gde smo koristili (M2), I.H. i (S1).

7) Indukcijom po y.

Za $y = \mathbf{1}$ imamo $x \cdot \mathbf{1} = \mathbf{1} \cdot x\ (= x)$ na osnovu 6). Neka sada važi $\forall x\ (x \cdot y = y \cdot x)$. Imamo $x \cdot y' = (x \cdot y) + x = (y \cdot x) + (\mathbf{1} \cdot x) = (y + 1) \cdot x = y' \cdot x$, gde smo koristili (M2), I.H., 6), 4) i (S1). □

Stav 4 $\forall x, y, z\ (x + z = y + z \Rightarrow x = y)$.

Dokaz. Indukcijom po z pokazujemo $\forall x, y\ (x + z = y + z \Rightarrow x = y)$.

– Za $z = \mathbf{1}$: $x + \mathbf{1} = y + \mathbf{1} \Rightarrow x' = y' \Rightarrow x = y$.

– Neka za broj z važi $\forall x, y\ (x + z = y + z \Rightarrow x = y)$. Imamo $x + z' = y + z' \Rightarrow (x + z)' = (y + z)' \Rightarrow x + z = y + z \Rightarrow$ I.H.: $x = y$. □

Stav 5 $\forall x, y\ (x \neq x + y)$.

Dokaz. Ako je $x = \mathbf{1}$ onda $x = x+y$ znači $\mathbf{1} = y'$, a ovo po prvoj Peanovoj aksiomi nije moguće. Ako je $x \neq \mathbf{1}$ onda na osnovu Stava 2 postoji $z \in P$ tako da je $x = z'$, pa iz $x = x + y$ sada sledi $z + \mathbf{1} = z + \mathbf{1} + y$, odnosno $\mathbf{1} = y'$ (nakon primene Stava 4) - što je nemoguće.

Stav 6 $\forall x, y, z\ (x \cdot z = y \cdot z \Rightarrow x = y)$.

Dokaz. Indukcijom po x.

– Za $x = \mathbf{1}$: Neka važi $\mathbf{1} \cdot z = y \cdot z$. Pokažimo da je $x = y$, tj. $y = \mathbf{1}$.

Kad bi bilo $y \neq \mathbf{1}$ onda $\exists a\ (y = a+\mathbf{1})$ pa $z = (a+\mathbf{1})\cdot z = (a\cdot z)+\mathbf{1}\cdot z = (a\cdot z)+z$ tj. $z = (a \cdot z) + z$, a ovo je nemoguće prema Stavu 5. Dakle mora biti $y = \mathbf{1}$.

– Neka za x važi $x \cdot z = y \cdot z \Rightarrow x = y$ i pretpostavimo $x' \cdot z = y \cdot z$, tj. $(x + \mathbf{1}) \cdot z = y \cdot z$ odnosno $x \cdot z + z = y \cdot z$.

Kad bi bilo $y = \mathbf{1}$ imali bi smo $x \cdot z + z = z$, što je nemoguće prema Stavu 5. Dakle mora biti $y \neq \mathbf{1}$. Zato $\exists u\ (y = u + \mathbf{1})$. Sada iz $x \cdot z + z = y \cdot z$ sledi

$x \cdot z + z = (u + \mathbf{1}) \cdot z = u \cdot z + z \Rightarrow\ x \cdot z = u \cdot z \Rightarrow$ I.H.: $x = u \Rightarrow\ x' = x + \mathbf{1} = u + \mathbf{1} = y$. □

Definicija 4 Za prirodne brojeve x i y definisaćemo da je $x < y$ ako postoji prirodan broj z tako da je $y = x + z$. Definišemo i "$x \leq y$" sa "$x < y \vee x = y$". $\square$

Stav 7 Relacija $\leq$ na strukturi prirodnih brojeva je relacija poretka.

Dokaz. *Refleksivnost.* Sledi direktno iz definicije.

Antisimetričnost. Neka je $x \leq y$ i $y \leq x$. Na osnovu definicije postoje četiri mogućnosti:
1) $x = y$ i $y = x$;
2) $x = y$ i $x = y + v$ za neko v;
3) $y = x + u$ za neko u i $y = x$;
4) $y = x + u$ za neko u i $x = y + v$ za neko v.

U slučajevima 1), 2) i 3) trivijalno važi $x = y$ (uzgred, slučajevi 2) i 3) nisu zapravo ni mogući - zašto?). U slučaju 4) imamo $(x+u)+v = x$ odnosno $x+(u+v) = x$, te na osnovu Stava 5 zaključujemo da je ovaj slučaj zapravo nemoguć.

Tranzitivnost. Neka važi $x \leq y$ i $y \leq z$. Na osnovu definicije postoje četiri mogućnosti:
1) $x = y$ i $y = z$;
2) $x = y$ i $z = y + v$ za neko v;
3) $y = x + u$ za neko u i $y = z$;
4) $y = x + u$ za neko u i $z = y + v$ za neko v.

Lako je videti da u slučajevima 1), 2) i 3) važi $x \leq z$. U slučaju 4) imamo $(x + u) + v = z$ tj. $z = x + (u + v)$ pa je ponovo $x \leq z$. $\square$

Stav 8 Uređenje "$\leq$" je linearno.

Dokaz. Indukcijom po x pokazujemo da važi $\forall y\ (x \leq y \vee y \leq x)$.

– Za $x = \mathbf{1}$: Treba pokazati da $\mathbf{1} \leq y \vee y \leq \mathbf{1}$. Ako je $y = \mathbf{1}$ onda je ovo trivijalno zadovoljeno a ako $y \neq \mathbf{1}$ onda postoji neko z tako da $y = z' = z + \mathbf{1} = \mathbf{1} + z$ odakle vidimo da je $\mathbf{1} \leq y$.

– Neka za x važi indukcijska hipoteza i neka je dat y. Pokažimo $x' \leq y \vee y \leq x'$. Po I.H. važi $x \leq y \vee y \leq x$ pa postoje tri mogućnosti:
1) $y = x + u$ za neko u;
2) $x = y + v$ za neko v;
3) $x = y$.

U slučaju 1) imamo da, ako je $u = \mathbf{1}$ onda $y = x'$ te $x' \leq y$, a ako je $u \neq \mathbf{1}$ onda $\exists w\ (u = w + \mathbf{1})$ pa je $y = x + w + \mathbf{1} = (x + \mathbf{1}) + w = x' + \mathbf{1}$ odakle se vidi da važi $x' \leq y$.

Analognim razmatranjem se pokazuje da u slučaju 2) važi $y' \leq x$.

Najzad, ako važi 3) onda je $y = x \leq x + \mathbf{1} = x'$. $\square$

Stav 9 "$\leq$" je *dobro* uređenje.

Dokaz. Neka je data s.p.b. $(P, \mathbf{1}, ')$. Na osnovu Stava 8 preostaje da se pokaže da ako je $A \subseteq P$ neprazan skup onda postoji $x \in A$ tako da $\forall y \in A\ (x \leq y)$. Neka je dat takav A.

Primetimo najpre da $\forall x\ (\mathbf{1} \leq x)$. Zaista ako je $x = \mathbf{1}$ onda $\mathbf{1} \leq x$ trivijalno važi, a ako je $x \neq \mathbf{1}$ onda postoji y tako da $x = y + \mathbf{1} = \mathbf{1} + y$ pa je opet $\mathbf{1} \leq x$.

Pretpostavimo suprotno, tj. da ne postoji $x \in A$ tako da je $\forall y \in A\ (x \leq y)$. Tada za $B := \{x | \forall y \in A\ (x \leq y)\}$ imamo $A \cap B = \emptyset$ i $\mathbf{1} \in B$. Pokažimo da za svako x važi $x \in B \Rightarrow x' \in B$.

Neka $x \in B$ i pretpostavimo da je $x' \notin B$. Tada postoji $y \in A$ tako da ne važi $x' \leq y$. Kako je $x \in B,\ y \in A$ to zaključujemo $x \leq y$ a iz $A \cap B = \emptyset$ dobijamo da $x \neq y$. Zato je $x < y$ tj. postoji neko v tako da $y = x + v$. Kad bi bilo $v = \mathbf{1}$ onda $y = x + \mathbf{1}$ tj. $x' = x + \mathbf{1} \leq y$, što je nemoguće. Dakle mora biti $v \neq \mathbf{1}$ pa je $v = u + \mathbf{1}$ za neko u. Zato je $y = x + u + \mathbf{1} = (x + \mathbf{1}) + u$ tj. $x + \mathbf{1} \leq y$, kontradikcija. Dakle mora biti $x' \in B$.

Na osnovu dokazanog dobijamo $B = P$ pa, zbog $A \cap B = \emptyset$, imamo $A = \emptyset$, suprotno polaznoj pretpostavci. $\square$

Stav 10 $x \leq y \Rightarrow (x + z \leq y + z\ \wedge\ x \cdot z \leq y \cdot z)$.

Dokaz. Sledi direktno iz definicije razlikujući slučajeve $x = y$ i $x < y$. $\square$

§

Dokaz Teoreme o rekurziji - varijanta koja ne koristi pojam prirodnog broja:

Definišimo skupove

$$\mathcal{F} := \{f | f \text{ je funkcija, } \mathbf{1} \in dom(f) \subseteq P,\ ran(f) \subseteq S,\ f(\mathbf{1}) = a_0$$

$$\text{i važi } x' \in dom(f) \Rightarrow (x \in dom(f) \wedge f(x') = T(x', f(x)))\}$$

i

$$U := \{x \in P | \exists f \in \mathcal{F}(x \in dom(f)) \text{ i važi da ako su } f, g \in \mathcal{F} \text{ takve}$$
$$\text{da } x \in dom(f) \cap dom(g) \text{ onda } f(x) = g(x)\}.$$

(1) Pokazujemo $\mathbf{1} \in U$. Definišimo $h : \{\mathbf{1}\} \to S$ sa $h(\mathbf{1}) := a_0$. Kako $\forall x \in P(\mathbf{1} \neq x')$ to $h \in \mathcal{F}$. Ako $f, g \in \mathcal{F}$ onda $f(\mathbf{1}) = g(\mathbf{1})(= a_0)$. Zato $\mathbf{1} \in U$.

(2) Pokazujemo $x \in U \Rightarrow x' \in U$. Neka $x_0 \in U$.

Postoji $f_0 \in \mathcal{F}$ tako da $x_0 \in dom(f_0)$. Označimo $A := dom(f_0) \cup \{x_0'\}$ i definišimo funkciju $g_0 : A \to S$ sa:

ako $y \in dom(f_0)$ onda $g_0(y) := f_0(y)$; ako $y \in A \setminus dom(f_0)$ onda $g_0(y) := T(x_0', f_0(x_0))$.

• Pokažimo da je $g_0 \in \mathcal{F}$.

- $\mathbf{1} \in dom(f_0) \subseteq A \equiv dom(g_0)$ i po definiciji preslikavanja g_0 je $g_0(\mathbf{1}) = f_0(\mathbf{1}) = a_0$.

- Neka je $z' \in dom(g_0)$ $(\equiv A)$.

Ako $z' \in dom(f_0)$ onda, zbog $f_0 \in \mathcal{F}$, $z \in dom(f_0)$ i $f_0(z') = T(z', f_0(z))$.

Odatle na osnovu definicije preslikavanja g_0, a zbog $z, z' \in dom(f_0)$, imamo $z \in dom(g_0)$ i $g_0(z') = T(z', g_0(z))$.

Ako $z' \notin dom(f_0)$ onda $z' = x_0'$, tj. $z = x_0 \in dom(f_0) \subseteq dom(g_0)$ pa, na osnovu definicije preslikavanja g_0, dobijamo $g_0(z') = T(x_0', f_0(x_0)) = T(z', g_0(z))$.

Dakle, $g_0 \in \mathcal{F}$. •

Upravo je pokazano da $x_0' \in dom(g_0)$ gde $g_0 \in \mathcal{F}$.

Neka $f_1, f_2 \in \mathcal{F}$ i $x_0' \in dom(f_1) \cap dom(f_2)$.

Pošto $f_i \in \mathcal{F}$ to $x_0 \in dom(f_i)$ i $f_i(x_0') = T(x_0', f_i(x_0))$, $i = \overline{1,2}$. Kako je $x_0 \in U$, $x_0 \in dom(f_1) \cap dom(f_2)$ i $f_1, f_2 \in \mathcal{F}$ to $f_1(x_0) = f_2(x_0)$ i najzad $f_1(x_0') = T(x_0', f_1(x_0)) = T(x_0', f_2(x_0)) = f_2(x_0')$.

U skladu sa prethodnim zaključujemo da je $x_0' \in U$.

Na osnovu (1), (2) i (P3) je $U = P$.

Definišimo traženo preslikavanje $k : P \to S$. Neka $x \in P$. Kako je $P = U$ to je skup $D_x := \{f(x) | f \in \mathcal{F},\ x \in dom(f)\}$ jednočlan. Definišimo $k(x) \in S$ sa $D_x = \{k(x)\}$.

– $P = U$ te postoji $f \in \mathcal{F}$ tako da $\mathbf{1} \in dom(f)$. Tada je $k(\mathbf{1}) = f(\mathbf{1}) = a_0$ (jer $f \in \mathcal{F}$).

– Neka $x \in P$. Imamo da je $k(x') = f(x')$ za neko (bilo koje) $f \in \mathcal{F}$, gde $x' \in dom(f)$. No tada je $x \in dom(f)$ i $f(x') = T(x', f(x))$, tj. $k(x') = T(x', k(x))$.

Dakle k zaista ima tražene osobine.

Dokažimo sada da je ovakvo preslikavanje jedinstveno.

Neka su $k, l : P \to S$ preslikavanja sa osobinama iz formulacije teoreme. $G := \{x \in P | k(x) = l(x)\}$. Imamo da $k(\mathbf{1}) = l(\mathbf{1}) = a_0$ pa je $\mathbf{1} \in G$. S druge strane ako $x \in G$ onda je $k(x) = l(x)$ pa je $k(x') = T(x', k(x)) = T(x', l(x)) = l(x')$, tj. $x' \in G$. Otuda je $G = P$, odnosno $k = l$. $\square$

Jedna od najvažnijih posledica Teoreme o rekurziji jeste činjenica da u suštini, ako se zanemari priroda elemenata u strukturama prirodnih brojeva, postoji tačno jedna takva struktura. Preciznije, imamo da važi sledeća

Teorema 2 Neka su $(P, \mathbf{1}, ')$ i $(P_0, \mathbf{1}_0, ^\dagger)$ strukture prirodnih brojeva. Tada postoji jedinstveno preslikavanje $f : P \to P_0$ sa osobinama:
– $f(\mathbf{1}) = \mathbf{1}_0$,
– $f(x') = (f(x))^\dagger$ za svako $x \in P$.
To jedinstveno f je usto i bijekcija.

Dokaz. (I) (Egzistencija i jedinstvenost) Definišimo $T : P \times P_0 \to P_0$ sa $T((x, y)) := y^\dagger$. Imajući u vidu da je $T(x', h(x)) = (h(x))^\dagger$ za proizvoljno $h : P \to P_0$ to, na osnovu teoreme o rekurziji, postoji tačno jedno preslikavanje $k : P \to P_0$ za koje važi
– $k(\mathbf{1}) = \mathbf{1}_0$,
– $k(x') = (k(x))^\dagger$ za svako $x \in P$.

(II) (Bijektivnost) Na osnovu upravo pokazanog postoji neko $k_0 : P_0 \to P$ tako da važi
– $k_0(\mathbf{1}_0) = \mathbf{1}$,
– $k_0(x^\dagger) = (k(x))'$ za svako $x \in P_0$.
Dokažimo da je $k_0 \circ k = id_P$. Neka $L := \{x \in P | (k_0 \circ k)(x) = x\}$.
$(k_0 \circ k)(\mathbf{1}) = k_0(k(\mathbf{1})) = k_0(\mathbf{1}_0) = \mathbf{1}$ pa je $\mathbf{1} \in L$.
Neka je sada $x \in L$, tj. $(k_0 \circ k)(x) = x$. $(k_0 \circ k)(x') = k_0(k(x')) = k_0((k(x))^\dagger) = (k_0(k(x)))' = ((k_0 \circ k)(x))' = x'$ te je $x' \in L$.
Zaključujemo da je $L = P$, tj. da $k_0 \circ k = id_P$, a odavde sledi da je k injektivno.
Na sličan način se pokazuje i da je $k \circ k_0 = id_{P_0}$ odakle zaključujemo da k mora da bude i "*na*" preslikavanje. $\square$

Dokaz Teoreme o rekurziji - varijanta koja koristi pojam prirodnog broja kao i postojanje nizova koji "*zadovoljavaju unapred date rekurzivne uslove*":

Tvrđenje Teoreme o rekurziji zadovoljava konkretna struktura $(\mathbb{N}, 1, h)$ gde je $h(n) = n + 1$. Zato će ga zadovoljavati i struktura $(P, \mathbf{1}, ')$ ako pokažemo da postoji neka bijekcija $a : \mathbb{N} \to P$ sa osobinama:

(1) $a(1) = \mathbf{1}$,
(2) $a(n+1) = a(n)'$ za svako $n \in \mathbb{N}$.

Neka je $a : \mathbb{N} \to P$ niz rekurzivno zadat sa (1) i (2). Skup $M := \{a(n) : n \in \mathbb{N}\}$ zadovoljava osobine $\mathbf{1} \in M$ i $x \in M \Rightarrow x' \in M$ pa je a preslikavanje *na*.

Indukcijom po $n \in \mathbb{N}$ pokazujemo: ako je $1 \leq i < j \leq n$ onda je $a(i) \neq a(j)$. Imamo $a(1) = \mathbf{1} \neq a(1)' = a(2)$ pa je tvrđenje tačno za $n = 2$. Pretpostavimo da je ono tačno za neko $n \geq 2$ i neka, suprotno onom što treba pokazati, skup $\{a(1), \ldots, a(n+1)\}$ ima manje od $n+1$ elemenata. Kako skup $\{a(1), \ldots, a(n)\}$ po indukcijskoj hipotezi ima n elemenata, to mora biti $a(n+1) = a(k)$ za neko $k \in \{1, \ldots, n\}$. Iz $a(1) = \mathbf{1} \neq a(n)' = a(n+1)$ sledi da je $k \geq 2$ pa je $k - 1 \in \mathbb{N}$. Zato sada iz $a(k-1)' = a(n)'$ sledi da je $a(k-1) = a(n)$, što protivureči indukcijskoj hipotezi.

(Primetimo da smo upravo zapravo dali i jedan dokaz Teoreme 2.)

□

I.2 Celi brojevi

Neka je data struktura prirodnih brojeva $(P, \mathbf{1}, ')$. Na skupu $P^2 = P \times P$ definišemo relaciju "$\sim$" sa

$$(a, b) \sim (c, d) \text{ akko } a + d = b + c.$$

Pokažimo da je "$\sim$" relacija ekvivalencije.

Refleksivnost. Imamo $a + b = b + a$ pa je $(a, b) \sim (a, b)$.

Simetričnost. Neka je $(a, b) \sim (c, d)$. Tada $a+d = b+c$ tj. $c+b = d+a$ odnosno $(c, d) \sim (a, b)$.

Tranzitivnost. Neka je $(a, b) \sim (c, d)$ i $(c, d) \sim (e, f)$. Tada je $a+d = b+c$ i $c+f = d+e$ pa sabiranjem ove dve jednakosti dobijamo $(a+f)+(c+d) = (b+e)+(c+d)$, odakle korišćenjem Stava 4 dobijamo $a + f = b + e$, tj. $(a, b) \sim (e, f)$.

Klase ekvivalencije ove relacije "$\sim$" zovemo *celim brojevima date strukture prirodnih brojeva*. Skup celih brojeva označimo sa

$$\mathbb{Z}(P, \mathbf{1}, ') = \mathbb{Z}(P) := P^2/\sim, .$$

Ako je $(m, n) \in P^2$ sa $[(m, n)]_\sim$ ćemo označavati klasu ekvivalencije para (m, n).

Stav 11 Neka je $(a, b) \sim (a_1, b_1)$ i $(c, d) \sim (c_1, d_1)$. Tada $(a + c, b + d) \sim (a_1 + c_1, b_1 + d_1)$.

Dokaz. Imamo da je $a + b_1 = b + a_1$ i $c + d_1 = d + c_1$. Sabiranjem dobijamo $(a + c) + (b_1 + d_1) = (b + d) + (a_1 + c_1)$, tj. $(a + c, b + d) \sim (a_1 + c_1, b_1 + d_1)$. □

Na osnovu Stava 11 operacija "$\oplus$" na skupu $\mathbb{Z}(P)$ određena sa

$$[(a, b)]_\sim \oplus [(c, d)]_\sim \ := \ [(a + c, b + d)]_\sim$$

je korektno definisana. Tu operaciju nazivamo *sabiranje celih brojeva* i nadalje ćemo je označavati sa "+" ukoliko je jasno iz konteksta na koju se operaciju, sabiranje prirodnih ili sabiranje celih brojeva, misli.

U nastavku ćemo za prirodne brojeve a i b umesto "$a \cdot b$" pisati "ab".

Stav 12 Neka je $(a, b) \sim (a_1, b_1)$ i $(c, d) \sim (c_1, d_1)$. Tada

$$(ad + bc, ac + bd) \sim (a_1d_1 + b_1c_1, a_1c_1 + b_1d_1).$$

Dokaz. Imamo da je $a + b_1 = b + a_1$ i $c + d_1 = d + c_1$. Izvedimo sledeći niz transformacija: prvu jednakost pomnožimo sa d; prvu pomnožimo sa c i zamenimo strane;

drugu pomnožimo sa a_1 i zamenimo strane; drugu pomnožimo sa b_1. Dobijamo, u tom redosledu, sledeće jednakosti:

$$\begin{aligned} ad + b_1 d &= bd + a_1 d \\ bc + a_1 c &= ac + b_1 c \\ da_1 + c_1 a_1 &= ca_1 + d_1 a_1 \\ cb_1 + d_1 b_1 &= db_1 + c_1 b_1. \end{aligned}$$

Sabiranjem ove četiri jednakosti dobija se

$$(ad + bc) + (a_1 c_1 + b_1 d_1) + (b_1 d + a_1 c + da_1 + cb_1) =$$

$$(ac + bd) + (a_1 d_1 + b_1 c_1) + (a_1 d + b_1 c + ca_1 + db_1)$$

odakle na osnovu Stava 4 dobijamo konačno

$$(ad + bc) + (a_1 c_1 + b_1 d_1) = (ac + bd) + (a_1 d_1 + b_1 c_1),$$

tj. $(ad + bc, ac + bd) \sim (a_1 d_1 + b_1 c_1, a_1 c_1 + b_1 d_1)$. □

Na osnovu Stava 12 imamo da je operacija "$\odot$" na skupu $\mathbb{Z}(P)$ zadata sa

$$[(a, b)]_\sim \odot [(c, d)]_\sim \ := \ [(ad + bc, ac + bd)]_\sim$$

korektno definisana. Nju nazivamo *množenje celih brojeva* a nadalje u pisanju najčešće izostavljamo oznaku "$\odot$" isto onako kako je to dogovoreno da se radi sa oznakom "$\cdot$" kod množenja prirodnih brojeva.

Stav 13 Operacije sabiranja i množenja celih brojeva su asocijativne i komutativne. Množenje je distributivno prema sabiranju.

Dokaz. Utvrđuje se direktnom proverom na osnovu definicije. □

Stav 14 $(\mathbb{Z}(P), +)$ je Abelova grupa.

Dokaz. Preostaje da se utvrdi postojanje neutrala i postojanje suprotnog elementa za svaki element skupa $\mathbb{Z}(P)$.

Imamo $(x, x) \sim (y, y)$ za svako $x, y \in P$. Takođe, ako je $(u, v) \sim (c, c)$ onda $u + c = v + c$ odnosno, posle skraćivanja, $u = v$. Zato je $[(x, x)]_\sim = [(y, y)]_\sim = \{(z, z) | z \in \mathbb{N}\}$. Označimo ovaj element skupa $\mathbb{Z}(P)$ sa $\mathbf{0}$.

$[(a, b)]_\sim + \mathbf{0} = [(a, b)]_\sim + [(c, c)]_\sim = [(a + c, b + c)]_\sim = [(a, b)]_\sim$ jer je očigledno $(a + c, b + c) \sim (a, b)$. Zato je $\mathbf{0}$ neutral za sabiranje.

$[(a, b)]_\sim + [(b, a)]_\sim = [(a + b, b + a)]_\sim = [(a + b, a + b)]_\sim = \mathbf{0}$ pa postoji suprotan element elementu $[(a, b)]_\sim$ u odnosu na sabiranje i to je $[(b, a)]_\sim$. □

Oznaka $\mathbf{0}$ će se i u daljem tekstu odnositi na neutralni element za sabiranje u $\mathbb{Z}(P)$ opisan u dokazu prethodne teoreme.

Suprotan element elementu $x \in \mathbb{Z}(P)$ u odnosu na sabiranje označavaćemo sa $-x$.

Primetimo da je $(n, n+\mathbf{1}) \sim (m, m+\mathbf{1})$ za proizvoljne $n, m \in P$. Takođe, ako je $(u, v) \sim (x, x+\mathbf{1})$ onda je $u + x + \mathbf{1} = v + x$, odnosno $u + \mathbf{1} = v$. Zato je $[(n, n+\mathbf{1})]_\sim = [(m, m+\mathbf{1})]_\sim = \{(x, x+\mathbf{1}) | x \in P\}$. Označimo ovaj element skupa $\mathbb{Z}(P)$ sa 1. Lako je videti da je on jedinični za množenje celih brojeva:

$$[(a, b)]_\sim [(n, n+\mathbf{1})]_\sim = [(an + bn + a, an + bn + b)]_\sim = [(a, b)]_\sim$$

jer je očigledno $(an + bn + a, an + bn + b) \sim (a, b)$.

Stav 15 Ako je $x \in \mathbb{Z}(P)$ i $x \neq \mathbf{0}$ onda za svako $y, z \in \mathbb{Z}(P)$ važi $xy = xz \Rightarrow y = z$.

Dokaz. Neka je $x = [(a, b)]_\sim \neq \mathbf{0}$, $y = [(c, d)]_\sim$, $z = [(e, f)]_\sim$ i neka važi

$$[(a, b)]_\sim \cdot [(c, d)]_\sim = [(a, b)]_\sim \cdot [(e, f)]_\sim$$

odnosno, prema definiciji

$$[(ad + bc, ac + bd)]_\sim = [(af + be, ae + bf)]_\sim$$

ili, drugim rečima

$$ad + bc + ae + bf = ac + bd + af + be. \qquad (*)$$

Kako je $x \neq \mathbf{0} = \{(n, n) | n \in P\}$, to je $a \neq b$. Neka je npr. $a < b$ (za slučaj $b < a$ dokaz je analogan), što znači da je $b = a + k$ za neko $k \in P$. Zamenjujući ovo u $(*)$ dobijamo:

$$ad + ac + kc + ae + af + kf = ac + ad + kd + af + ae + ke$$

odnosno $k(c + f) = k(d + e)$ i najzad $c + f = d + e$, što znači da je $(c, d) \sim (e, f)$, tj. $y = z$. $\square$

Na osnovu prethodno ustanovljenih činjenica u vezi sa strukturom $(\mathbb{Z}(P), \oplus, \odot)$ možemo konstatovati da je $(\mathbb{Z}(P), \oplus, \odot)$ *integralni domen.*

Uočimo skup $P^* := \{[(x, y)]_\sim \in \mathbb{Z}(P) | \ \ x, y \in P, \ x < y\}$ i preslikavanje $CB : P \to \mathbb{Z}(P)$ definisano sa $CB(n) := [(\mathbf{1}, \mathbf{1} + n)]_\sim$.

Stav 16 Preslikavanje CB je injektivno i $CB[P] = P^*$.

Dokaz. Neka $CB(n) = CB(m)$ za $n, m \in P$. Ovo znači da je $(\mathbf{1}, \mathbf{1}+n) \sim (\mathbf{1}, \mathbf{1}+m)$ odnosno da $\mathbf{1} + \mathbf{1} + m = \mathbf{1} + n + \mathbf{1}$, tj. $m = n$. Dakle CB je injektivno.

Jasno je da $\mathbf{1} < \mathbf{1} + n$ pa je $CB(n) \in P^*$, tj. važi $CB[P] \subseteq P^*$.

Uočimo proizvoljno $a \in P^*$. Postoje $x, y \in P$, pri čemu $x < y$, tako da je $a = [(x, y)]_\sim$. Postoji $k \in P$ tako da $y = x + k$. Ako je $x = \mathbf{1}$ onda dobijamo $(x, y) = (\mathbf{1}, \mathbf{1} + k)$ tj. $a = CB(k)$. Ako je $x \neq \mathbf{1}$ tada postoji $u \in P$ tako da $x = u + \mathbf{1}$ pa imamo da $(x, y) = (u + \mathbf{1}, u + \mathbf{1} + k) \sim (\mathbf{1}, \mathbf{1} + k)$, tj. $a = CB(k)$. Odavde vidimo da je $P^* \subseteq CB[P]$. □

Stav 17 Za svako $n, m \in P$ je $CB(n + m) = CB(n) + CB(m)$ i $CB(nm) = CB(n)CB(m)$.

Dokaz. Sledi direktnom proverom. □

Definicija 5 Na $\mathbb{Z}(P)$ definišemo relaciju "$<$" sa

$$x < y \text{ ako i samo ako } \exists z \in P^* \ (y = x + z).$$

Relacija "$\leq$" na skupu $\mathbb{Z}(P)$ se definiše uobičajeno: $x \leq y$ akko $x = y \vee x < y$. □

Stav 18 Za svako $x, y \in P$ je $x < y \iff CB(x) < CB(y)$. Za svako $x, y \in P$ je $x \leq y \iff CB(x) \leq CB(y)$.

Dokaz. Neka je $x, y \in P$ i $x < y$. Tada $\exists k \in P$ tako da $y = x + k$. Odavde na osnovu Stava 17 imamo da je $CB(y) = CB(x) + CB(k)$ pri čemu je $CB(k) \in P^*$ po Stavu 16, te vidimo da je $CB(x) < CB(y)$.

Neka sada $CB(x) < CB(y)$. Tada postoji $z \in P^*$ tako da $CB(y) = CB(x) + z$. Na osnovu Stava 16 postoji $k \in P$ tako da je $z = CB(k)$. Zato je $CB(y) = CB(x) + CB(k) = CB(x + k)$, po Stavu 17, a kako je CB injektivno zaključujemo da je $y = x + k$, tj. $x < y$.

Preostali deo tvrđenja sada sledi neposredno. □

Stav 19 Relacija "$\leq$" je linearno uređenje na skupu $\mathbb{Z}(P)$.

Dokaz. *Refleksivnost* sledi direktno iz definicije.

Antisimetričnost. Neka važi $x \leq y$ i $y \leq x$.

Pretpostavimo najpre da je $x < y$ i $y < x$. Tada postoje $u, v \in P^*$ tako da je $y = x + v$ i $x = y + u$. Zato je $y = (y + u) + v$ pa je $\mathbf{0} = u + v$, tj. $u = -v$. Ako je $u = [(\mathbf{1}, \mathbf{1}+n)]_\sim$ i $v = [(\mathbf{1}, \mathbf{1}+m)]_\sim$ za neke $n, m \in P$ imamo da je $-v = [(\mathbf{1}+m, \mathbf{1})]_\sim$ (vidi dokaz Stava 14) pa dobijamo $(\mathbf{1}+m, \mathbf{1}) \sim (\mathbf{1}, \mathbf{1}+n)$ odnosno $m+\mathbf{1}+\mathbf{1}+n = \mathbf{1}+\mathbf{1}$ odakle je $\mathbf{1} = m + n + \mathbf{1} = (m + n)'$ kontradikcija. Zato ne može biti istovremeno i $x < y$ i $y < x$, odakle neposredno zaključujemo da je $x = y$.

Tranzitivnost. Neka je $x \leq y$ i $y \leq z$. Jedini slučaj kada je uopšte i potrebno nešto dokazivati jeste slučaj $x < y \wedge y < z$ pa pretpostavimo da se o njemu i radi. Postoje $n, m \in P^*$ tako da je $y = x + n$ i $z = y + m$. Tada je $z = x + (n + m)$. Odavde sledi da je $x < z$ jer je $n + m \in P^*$: $n = CB(p)$, $m = CB(q)$ za neke $p, q \in P$ po Stavu 16, pa je $n + m = CB(p) + CB(q) = CB(p + q)$ po Stavu 17, tj. $n + m \in CB[P] = P^*$.

Pokažimo najzad da su x i y iz $\mathbb{Z}(P)$ uvek uporedivi. Dakle, neka je $x = [(a, b)]_\sim$, $y = [(c, d)]_\sim$ i pretpostavimo da je $x \neq y$. Tada je $a + d \neq b + c$, tj. $l \neq r$ gde $l := a + d$ i $r := b + c$. Zato je $l < r$ ili $r < l$ jer je "$\leq$" na skupu P linearno. Pretpostavimo da je $l < r$ (preostali slučaj je analogan), tj. da postoji $k \in P$ tako da je $r = l + k$ odnosno $b + c = a + d + k$. Odavde sledi da je

$$b + c + \mathbf{1} = a + d + k + \mathbf{1}$$

te je $x = [(a, b)]_\sim = [(c + \mathbf{1}, d + k + \mathbf{1})]_\sim = [(c, d)]_\sim + [(\mathbf{1}, \mathbf{1} + k)]_\sim$, tj. $x = y + z$ gde je $z := [(\mathbf{1}, \mathbf{1} + k)]_\sim \in P^*$. Drugim rečima $y < x$. □

Stav 20 $x < y \Rightarrow -y < -x$ za svako $x, y \in \mathbb{Z}(P)$.

Dokaz. Neka $x < y$. Tada postoji $k \in P^*$ tako da $y = x + k$. Zato $-y = -x + (-k)$ odnosno $-x = (-y) + k$, što znači da je $-y < -x$. □

Stav 21 Za svako $x, y, z \in \mathbb{Z}(P)$ važi $x \leq y \Rightarrow x + z \leq y + z$. □

Stav 22 Ako je $\mathbf{0} < a$ i $x < y$ onda $ax < ay$.

Dokaz. Iz $x < y$ imamo da je $y = x + k$ za neko $k \in \mathbb{N}^*$. Zato je $ay = ax + ak$ te bi $ax < ay$ sledilo ako se pokaže da je $ak \in P^*$: $\mathbf{0} < a$ znači da je $a \in P^*$ pa je zato $a = CB(a_1)$ i $k = CB(k_1)$ za neke $a_1, k_1 \in P$; otuda $ak = CB(a_1) \cdot CB(k_1) = CB(a_1 k_1) \in P^*$. □

Stav 23 U skupu celih brojeva (date strukture prirodnih brojeva) važi:
(1) $x, y > \mathbf{0} \;\Rightarrow\; (x + y > \mathbf{0} \;\wedge\; xy > \mathbf{0})$
(2) $x, y < \mathbf{0} \;\Rightarrow\; xy > \mathbf{0}$
(3) $(x > \mathbf{0} \wedge y < \mathbf{0}) \;\Rightarrow\; xy < \mathbf{0}$. □

Definišemo $\mathbb{Z}_+(P) := P^*,\ \mathbb{Z}_-(P) := \{-x|\ x \in \mathbb{Z}_+(P)\}$.
Jednostavno je pokazati da je $\mathbb{Z}_+(P) = \{x \in \mathbb{Z}(P)|\mathbf{0} < x\}$, $\mathbb{Z}_-(P) = \{x \in \mathbb{Z}|x < \mathbf{0}\}$ i $\mathbb{Z}_+(P) \cap \mathbb{Z}_-(P) = \emptyset$ kao i da važi $\mathbb{Z}(P) = \mathbb{Z}_-(P) \cup \{\mathbf{0}\} \cup \mathbb{Z}_+(P)$.

I.3 Racionalni brojevi

Neka je data struktura prirodnih brojeva $(P, \mathbf{1}, ')$ U ovom odeljku ćemo sa "0" (umesto sa "$\mathbf{0}$") označavati nulu prstena $\mathbb{Z}(P)$.

Na skupu $(\mathbb{Z}(P) \setminus \{0\}) \times \mathbb{Z}(P)$ definišimo relaciju "$\approx$" sa

$$(a, b) \approx (c, d) \quad \text{akko} \quad ad = bc.$$

"$\approx$" je relacija ekvivalencije. Klase ekvivalencije ove relacije nazivamo *racionalnim brojevima date strukture prirodnih brojeva* a skup svih racionalnih brojeva označavaćemo sa

$$\mathbb{Q}(P, \mathbf{1}, ') = \mathbb{Q}(P) := \Big((\mathbb{Z}(P) \setminus \{0\}) \times \mathbb{Z}(P)\Big) / \approx \ .$$

Stav 24 Neka je $(a, b) \approx (a_1, b_1)$ i $(c, d) \approx (c_1, d_1)$. Tada važi:

$$(ac, ad + bc) \approx (a_1c_1, a_1d_1 + b_1c_1)$$

i

$$(ac, bd) \approx (a_1c_1, b_1d_1).$$

Dokaz. Sledi iz pretpostavke $ab_1 = a_1b \ \wedge \ cd_1 = c_1d$ i definicije relacije "$\approx$". $\square$

Prethodni stav dozvoljava da se definišu sabiranje racionalnih brojeva sa

$$[(a, b)]_\approx + [(c, d)]_\approx := [(ac, ad + bc)]_\approx$$

i množenje racionalnih brojeva sa

$$[(a, b)]_\approx \cdot [(c, d)]_\approx := [(ac, bd)]_\approx.$$

Konvencija Umesto " $[(x, y)]_\approx$ " pisaćemo " $\dfrac{y}{x}$ ".

Stav 25 Za svako $x, y \in \mathbb{Z}(P)$ i svako $z, t \in \mathbb{Z}(P) \setminus \{0\}$ važi:

1) $\dfrac{xz}{tz} = \dfrac{x}{t}$;

2) $\dfrac{x + y}{z} = \dfrac{x}{z} + \dfrac{y}{z}$.

Dokaz. Tvrđenja slede direktnom proverom, npr.:
$\frac{x}{z} + \frac{y}{z} = \frac{xz+yz}{z\cdot z}$ a sada se lako vidi da je $(z\cdot z, xz+yz) \approx (z, x+y)$. $\square$

Stav 26 $(\mathbb{Q}(P), +, \cdot)$ je polje.

Dokaz. Sledi direktnom proverom uz korišćenje Stava 25. Istaknimo da je nula ovog polja $\frac{0}{1}$, suprotni element (za sabiranje) elementa $\frac{x}{y}$ je $\frac{(-x)}{y}$, jedinica ovog polja je $\frac{1}{1}$ a inverzni element (u odnosu na množenje) elementa $\frac{x}{y} \neq \frac{0}{1}$ je $\frac{y}{x}$ (gde ne može biti $x = 0$ jer bi tada imali $(y, x) \approx (1, 0)$). $\square$

Za $u \in \mathbb{Q}(P)$ kažemo da je *pozitivan* ako za svako $(a, b) \in u$ važi $ab > 0$. Definišimo $\mathbb{Q}_+(P) := \{ \frac{b}{a} \,|a, b \in \mathbb{Z}(P),\ ab > 0\}$.

Neka je $\frac{b}{a} = \frac{d}{c}$ i neka $ab > 0$. Pokažimo da mora biti i $cd > 0$.

Imamo da je $ad = bc$. Stav 23 kaže da je $a, b > 0$ ili $a, b < 0$. Neka važi $a, b > 0$, pri čemu se u preostalom slučaju rezonuje identično.
Iz $cd = 0$, zbog $c \neq 0$, sledi $d = 0$ a onda $bc = 0$ pa $b = 0$ te i $ab = 0$, što je nemoguće.
Iz $cd < 0$, na osnovu Stava 23, sledi $c > 0,\ d < 0$ ili $c < 0,\ d > 0$. U prvom slučaju dobijamo $bc > 0$ i $ad < 0$ a u drugom $bc < 0$ i $ad > 0$. Dakle, u oba slučaja je $ad = bc \in \mathbb{Z}_+(P) \cap \mathbb{Z}_-(P) = \emptyset$.

Prema tome važi jedini preostali slučaj.

Upravo utvrđena činjenica govori da je $u \in \mathbb{Q}(P)$ pozitivan akko postoji neko $(a, b) \in u$ tako da je $ab > 0$. U skladu s tim je $\mathbb{Q}_+(P) \equiv \{u \in \mathbb{Q}(P) |\ u \text{ je pozitivan}\}$.

Definišemo da za dva racionalna broja x, y važi $x < y$ akko $y - x \in \mathbb{Q}_+(P)$. Lako je videti da važi $x \in \mathbb{Q}_+(P) \iff x > \frac{0}{1}$. Kao i ranije, $x \leq y$ skraćuje $x = y \vee x < y$.

Stav 27 Ako je $x, y \in \mathbb{Q}(P)$ onda:
1) $x > \frac{0}{1} \iff -x < \frac{0}{1}$;
2) $x, y > \frac{0}{1} \Rightarrow x + y, xy > \frac{0}{1}$;

3) $x, y < \frac{0}{1} \Rightarrow x + y < \frac{0}{1} \wedge xy > \frac{0}{1}$;
4) $x > \frac{0}{1},\ y < \frac{0}{1} \Rightarrow xy < \frac{0}{1}$.

Dokaz. 1) $x > \frac{0}{1} \iff x - \frac{0}{1} \in \mathbb{Q}_+(P) \iff x \in \mathbb{Q}_+(P)$. S druge strane $-x < \frac{0}{1} \iff \frac{0}{1} - (-x) \in \mathbb{Q}_+(P) \iff x \in \mathbb{Q}_+(P)$.

2) Neka $x = \frac{b}{a}$ i $y = \frac{d}{c}$. $x, y > \frac{0}{1}$ znači da je $x, y \in \mathbb{Q}_+(P)$, tj. $ab, cd > 0$. Kako je $a, c \neq 0$ to je lako pokazati da je $a^2, c^2 > 0$. Otuda $abc^2 > 0$ i $a^2cd > 0$ pa je $abc^2 + a^2cd > 0$, tj. $ac(bc + ad) > 0$. Zato je $x + y = \frac{bc + ad}{ac} \in \mathbb{Q}_+(P)$ odnosno $x + y > \frac{0}{1}$.

Na osnovu Stava 23 imamo da je $abcd > 0$, tj. $xy - \frac{0}{1} = xy = \frac{bd}{ac} \in \mathbb{Q}_+(P)$, što znači da $xy > \frac{0}{1}$.

3) Ako je $x, y < \frac{0}{1}$ onda je, na osnovu 1), $-x, -y > \frac{0}{1}$, pa zbog 2) imamo $-x + (-y),\ (-x)(-y) > \frac{0}{1}$, tj. $xy > \frac{0}{1}$ i $-(x + y) > \frac{0}{1}$, te koristeći 1) dobijamo i $x + y < \frac{0}{1}$.

4) se slično dokazuje. □

Stav 28 Relacija "$\leq$" je linearno uređenje na skupu $\mathbb{Q}(P)$.

Dokaz. Refleksivnost sledi iz same definicije.

Neka važi $x \leq y$ i $y \leq x$. Kad ne bi važilo $x = y$ onda bi imali $x < y \wedge y < x$. Neka dakle $\{y - x,\ x - y\} \subseteq \mathbb{Q}_+(P)$. Iz $y - x > \frac{0}{1}$ i $x - y > \frac{0}{1}$ sledi $(y - x) + (x - y) > \frac{0}{1}$, tj. $\frac{0}{1} \in \mathbb{Q}_+(P)$. Odatle sledi $0 = 0 \cdot 1 > 0$, što je jednostavno proveriti da ne može da važi.

Neka je sada $x \leq y$ i $y \leq z$. Ako je $x = y$ ili $y = z$ onda direktno sledi $x \leq z$. Neka je $x \neq y \neq z$. Imamo da je $x < y$ i $y < z$, tj. $y - x > \frac{0}{1}$ i $z - y > \frac{0}{1}$. Odatle se dobija $z - x = (z - y) + (y - x) > \frac{0}{1}$, tj. $x < z$.

Neka je sada $x, y \in \mathbb{Q}(P)$. Pokažimo da su x i y uporedivi.

Neka je $y - x = \frac{b}{a}$. Razlikujemo tri slučaja: $ab = 0$, $ab < 0$ i $ab > 0$ (odgovarajuće uređenje na $\mathbb{Z}(P)$ je linearno).

U prvom slučaju dobijamo da je $b = 0$, tj. $y - x = \frac{0}{1}$, pa su x i $y = x$ uporedivi. U drugom slučaju imamo $-(ab) > 0$, tj. $a(-b) > 0$. Zato je $x - y = -\frac{b}{a} = \frac{-b}{a} \in \mathbb{Q}_+(P)$ pa je $y < x$. U trećem slučaju jasno važi $x < y$. □

Stav 29 Za svako $x, y, z \in \mathbb{Q}(P)$ važi
1) $x < y \Rightarrow x + z < y + z$;
2) Ako je $z > 0$ onda $x < y \Rightarrow xz < yz$.

Dokaz. 1) $x < y \Rightarrow (y+z) - (x+z) = y - x > \frac{0}{1}$, tj. $x + z < y + z$.
Tvrđenje pod 2) sledi direktno iz $y - x > \frac{0}{1}$ i Stava 27. □

Stav 30 Definišimo $RC : \mathbb{Z}(P) \to \mathbb{Q}(P)$ sa $RC(x) := \frac{x}{1}$.
1) RC je injektivno preslikavanje;
2) $RC(x + y) = RC(x) + RC(y)$;
3) $RC(xy) = RC(x)RC(y)$;
4) $x < y \iff RC(x) < RC(y)$.

Dokaz. 1) Neka je $RC(x) = RC(y)$. Tada $\frac{x}{1} = \frac{y}{1}$ pa je $(1, x) \approx (1, y)$, tj. $x = y$.
2) $RC(x + y) = \frac{x+y}{1} = \frac{x}{1} + \frac{y}{1} = RC(x) + RC(y)$.
3) $RC(xy) = \frac{xy}{1} = \frac{xy}{1 \cdot 1} = \frac{x}{1} \cdot \frac{y}{1} = RC(x) \cdot RC(y)$.
4) Neka važi $x < y$, tj. $y = x + k$ za neko $k \in P^*$. Tada $RC(y) = RC(x + k) = RC(x) + RC(k)$. Preostaje da se pokaže da je $\frac{k}{1} \equiv RC(k) \in \mathbb{Q}_+(P)$ ali ovo direktno sledi iz $k \cdot 1 = k \in P^* = \mathbb{Z}_+(P) = \{a \in \mathbb{Z}(P) | 0 < a\}$.

Neka sada važi $RC(x) < RC(y)$. Kako su celi brojevi x i y "$\leq$"-uporedivi, a kako je očigledno $x \neq y$, to je dovoljno pokazati da ne važi $y < x$. Kad bi to važilo na osnovu upravo pokazanog bi imali da je $RC(y) < RC(x)$. Dakle $RC(y) - RC(x) > \frac{0}{1}$ i $RC(x) - RC(y) > \frac{0}{1}$ pa sabiranjem ovih nejednakosti (preciznije: na osnovu Stava 27) dobijamo $\frac{0}{1} > \frac{0}{1}$, tj. $\frac{0}{1} \in \mathbb{Q}_+(P)$, odnosno $0 = 0 \cdot 1 > 0$, što je jednostavno pokazati da je nemoguće. □

Stav 31 Uređenje "$<$" na skupu racionalnih brojeva je gusto.

Dokaz. Neka su $p, q \in \mathbb{Q}(P)$, $p < q$. Treba pokazati da postoji $x \in \mathbb{Q}(P)$ tako da je $p < x < q$. Neka je $2 := 1 + 1 \in \mathbb{Z}(P)$ i $x := \frac{1}{2}(p + q)$.

Primetimo najpre da je na osnovu Stava 25: $\frac{1}{1} - \frac{1}{2} = \frac{2}{2} + \frac{(-1)}{2} = \frac{2-1}{2} = \frac{(1+1)-1}{2} = \frac{1}{2}$ kao i da je $\frac{1}{2} > \frac{0}{1}$ jer $1 \cdot 2 = 2 = 1 + 1 = CB(\mathbf{1}) + CB(\mathbf{1}) = CB(\mathbf{1} + \mathbf{1}) \in P^* = \mathbb{Z}_+(P)$, pa je $1 \cdot 2 > 0$.

Imamo $q - x = q - \frac{1}{2} \cdot p - \frac{1}{2} \cdot q = \frac{1}{1} \cdot q - \frac{1}{2} \cdot q - \frac{1}{2} \cdot p = (\frac{1}{1} - \frac{1}{2})q + \frac{1}{2}(-p) = \frac{1}{2}(q - p) > \frac{0}{1}$ na osnovu Stava 27 jer je $p < q$ i $\frac{1}{2} > \frac{0}{1}$. Zato je $x < q$. Slično se utvrđuje da je i $p < x$. □

I.4 Realni brojevi

Neka je data struktura prirodnih brojeva $(P, \mathbf{1}, ')$. Za $x \in \mathbb{Q}(P)$ definišemo

$$|x| := \begin{cases} x, & \text{ako je } x \geq \frac{0}{1}, \\ -x, & \text{ako je } x < \frac{0}{1}. \end{cases}$$

Za "*niz*" $a : P \to \mathbb{Q}(P)$ racionalnih brojeva date strukture prirodnih brojeva kažemo da je *Košijev* ako važi

$$\forall n \in P \exists m \in P \forall k, l \in P \left(m \leq k, l \Rightarrow |a(k) - a(l)| \leq \frac{1}{CB(n)} \right).$$

Označimo sa $\mathcal{R}$ skup svih Košijevih nizova racionalnih brojeva i na tom skupu definišimo relaciju $\cong$ sa

$$a \cong b \iff \forall n \in P \exists m \in P \forall k \in P \left(m \leq k \Rightarrow |a(k) - b(k)| \leq \frac{1}{CB(n)} \right).$$

Može se pokazati da je $\cong$ relacija ekvivalencije na skupu $\mathcal{R}$. Skup $\mathcal{R}/\cong$ svih klasa ekvivalencije ove relacije označimo sa $\mathbb{R}(P)$ a njegove elemente nazovimo *realnim brojevima*. Za $a \in \mathcal{R}$ sa $[a]_\cong$ označimo klasu niza a. Na skupu $\mathbb{R}(P)$ definišimo operacije

$$[a]_\cong + [b]_\cong := [a + b]_\cong, \quad [a]_\cong \cdot [b]_\cong := [a \cdot b]_\cong,$$

i relaciju $<$ sa

$$[a]_\cong < [b]_\cong \iff [a]_\cong \neq [b]_\cong \wedge \exists n \in \mathbb{N} \forall k \in \mathbb{N} \ (\ n \leq k \Rightarrow \ a(k) < b(k) \ ).$$

Može se pokazati da su ove definicije korektne (tj. da ne zavise od izbora predstavnika). Kao i obično: $x \leq y \iff x < y \vee x = y$ za $x, y \in \mathbb{R}(P)$.

Definicija 6 Za strukturu $(A, +, \cdot, \leq)$ kažemo da je *kompletno uređeno polje* ako je $(A, +, \cdot)$ polje, $\leq$ linearno uređenje na skupu A i, ako je a_0 nula tog polja, važe uslovi
(1) $x \leq y \Rightarrow x + z \leq y + z$,
(2) $(x \leq y \wedge a_0 \leq z) \Rightarrow x \cdot z \leq y \cdot z$ i
(3) svaki odozgo ograničen podskup od A ima supremum. □

Stav 32 Struktura $(\mathbb{R}(P), +, \cdot, \leq)$ je kompletno uređeno polje. □

O tome da su realni brojevi u potpunosti određeni svojom ovakvom relacijsko-operacijskom strukturom govori sledeća teorema.

Teorema 3 Za svaka dva $(A, +, \cdot, \leq)$ i $(B, \oplus, \odot, \preceq)$ kompletno uređena polja postoji bijekcija $f : A \to B$ tako da važi
(1) $f(x + y) = f(x) \oplus f(y)$,
(2) $f(x \cdot y) = f(x) \odot f(y)$,
(3) $x \leq y \iff f(x) \preceq f(y)$. $\square$

Pomenimo da su nula i jedinica polja $(\mathbb{R}(P), +, \cdot)$ klase ekvivalencije, tim redom, nizova $\langle 0|\ n \in\ P\rangle$ i $\left\langle 1 + \left.\dfrac{1}{CB(n)}\right|\ n \in P\right\rangle$.

Klase konstantnih nizova "*glume*" racionalne brojeve:

Stav 33 Preslikavanje $\mathrm{Real} : \mathbb{Q}(P) \to \mathbb{R}(P)$ definisano sa $\mathrm{Real}(x) := [\langle x|\ n \in \mathbb{N}\rangle]_{\cong}$ je injektivno i važi
(1) $\mathrm{Real}(x + y) = \mathrm{Real}(x) + \mathrm{Real}(y)$,
(2) $\mathrm{Real}(x \cdot y) = \mathrm{Real}(x) \cdot \mathrm{Real}(y)$,
(3) $x \leq y \iff \mathrm{Real}(x) \leq \mathrm{Real}(y)$ i
(4) ako su $x, y \in \mathbb{R}(P)$ različiti realni brojevi takvi da je $x \leq y$ tada postoji $z \in \mathrm{Real}[\mathbb{Q}(P)] \setminus \{x, y\}$ tako da je $x \leq z \leq y$. $\square$

I.5 Kompleksni brojevi

Za datu strukturu prirodnih brojeva $(P, \mathbf{1}, ')$ na skupu $\mathbb{C}(P) := \mathbb{R}(P)^2$ definišimo operacije

$$(a,b) + (c,d) := (a+c, b+d), \quad (a,b) \cdot (c,d) := (ac - bd, ad + bc).$$

Neka u ovom odeljku simboli 0 i 1 označavaju, redom, nulu i jedinicu polja realnih brojeva.

Stav 34 $(\mathbb{C}(P), +, \cdot)$ je polje. □

Elemente ovog polja nazivamo *kompleksnim brojevima*. Nula ovog polja je $(0,0)$ a jedinica $(1,0)$. Kompleksan broj $\mathbf{i} := (0,1)$ se naziva *imaginarna jedinica* i za njega važi $\mathbf{i}^2 = (-1,0) = -(1,0)$.

Ovo polje je proširenje polja realnih brojeva što je sadržaj narednog stava.

Stav 35 Preslikavanje $f : \mathbb{R}(P) \to \mathbb{C}(P)$ definisano sa $f(x) := (x,0)$ je injektivno i važi:
(1) $f(x+y) = f(x) + f(y)$, i
(2) $f(x \cdot y) = f(x) \cdot f(y)$. □

Kompletno uređenje polja realnih brojeva se ne može proširiti na polje kompleksnih brojeva. Štaviše

Stav 36 Ne postoji linearno uređenje na skupu $\mathbb{C}(P)$ za koje bi važilo
(1) $x \leq y \;\Rightarrow\; x + z \leq y + z$ i
(2) $(x \leq y \wedge (0,0) \leq z) \;\Rightarrow\; x \cdot z \leq y \cdot z$.

Dokaz. Neka je $\leq$ takvo uređenje. Zbog linearnosti ovog uređenja brojevi $(0,0)$ i imaginarna jedinica su uporedivi.

Ako je $(0,0) \leq \mathbf{i}$ onda $(0,0) = (0,0) \cdot \mathbf{0} \leq \mathbf{i} \cdot \mathbf{i}$, tj. $(0,0) \leq (-1,0)$.

Ako je $\mathbf{i} \leq (0,0)$ onda je $\mathbf{i} + (-\mathbf{i}) \leq (0,0) + (-\mathbf{i})$ tj. $(0,0) \leq -\mathbf{i}$. Odavde imamo $(0,0) \cdot (-\mathbf{i}) \leq (-\mathbf{i}) \cdot (-\mathbf{i})$, tj. $(0,0) \leq (-1,0)$.

Dakle, u svakom slučaju važi $(0,0) \leq (-1,0)$ pa sledi da je $(0,0) = (0,0) \cdot (-1,0) \leq (-1,0) \cdot (-1,0)$, tj. $(0,0) \leq (1,0)$. Zato je $(0,0) + (-1,0) \leq (1,0) + (-1,0)$ odnosno $(-1,0) \leq (0,0)$. Antisimetričnost relacije $\leq$ sada povlači $(0,0) = (-1,0)$, kontradikcija. □

Deo II

Elementi kombinatorike

II.1 Formula uključenja-isključenja

Notacija Za $i \in \mathbb{N}$ i proizvoljan skup M definišemo $M^{(i)} :\overset{\text{df}}{=} \{S \subseteq M \mid |S| = i\}$. Takođe, za proizvoljan konačan skup M sa $|M|$ označavamo broj njegovih elemenata.

Teorema 4 (*Formula uključenja-isključenja*) Za svako $n \in \mathbb{N}$ važi

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} \left\{ (-1)^{i+1} \sum_{S \in \{1,\ldots,n\}^{(i)}} \left| \bigcap_{j \in S} A_j \right| \right\},$$
$$\text{kad god su } A_i,\ 1 \leq i \leq n,\ \text{konačni skupovi.} \tag{II.1}$$

Dokaz. Indukcijom po n. Za $n \in \{1, 2\}$ tačnost tvrđenja se direktno proverava. Neka (II.1) važi za neki prirodan broj $n > 2$.

Zbog $\bigcup_{i=1}^{n+1} A_i = \bigcup_{i=1}^{n} (A_i \cup A_{n+1})$ imamo:

$$\left| \bigcup_{i=1}^{n+1} A_i \right| = \left| \bigcup_{i=1}^{n} (A_i \cup A_{n+1}) \right| = \sum_{i=1}^{n} \left\{ (-1)^{i+1} \sum_{S \in \{1,\ldots,n\}^{(i)}} \left| \bigcap_{j \in S} (A_j \cup A_{n+1}) \right| \right\} =$$

$$\left[\text{koristimo: } \left| \bigcap_{j \in S} (A_j \cup A_{n+1}) \right| = \left| A_{n+1} \cup \bigcap_{j \in S} A_j \right| = \right.$$

$$\left. = |A_{n+1}| + \left| \bigcap_{j \in S} A_j \right| - \left| A_{n+1} \cap \bigcap_{j \in S} A_j \right| \right]$$

$= K + L + M$, gde je

$$K := \sum_{i=1}^{n} \left\{ (-1)^{i+1} \sum_{S \in \{1,\ldots,n\}^{(i)}} | \ A_{n+1} \ | \right\} = |A_{n+1}| \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} = |A_{n+1}|,$$

$$L := \sum_{i=1}^{n} \left\{ (-1)^{i+1} \sum_{S\in\{1,\dots,n\}^{(i)}} \left| \bigcap_{j\in S} A_j \right| \right\} = \sum_{1\le j\le n} |A_j| + \\ + \sum_{i=2}^{n} \left\{ (-1)^{i+1} \sum_{S\in\{1,\dots,n\}^{(i)}} \left| \bigcap_{j\in S} A_j \right| \right\},$$

i

$$M := \sum_{i=1}^{n} \left\{ (-1)^{i+2} \sum_{S\in\{1,\dots,n\}^{(i)}} \left| \left(\bigcap_{j\in S} A_j \right) \cap A_{n+1} \right| \right\} = \\ = \sum_{i=2}^{n+1} \left\{ (-1)^{i+1} \sum_{\substack{S\in\{1,\dots,n+1\}^{(i)} \\ \setminus S\in\{1,\dots,n\}^{(i)}}} \left| \bigcap_{j\in S} A_j \right| \right\} = \\ = (-1)^{n+2} \left| \bigcap_{j\in\{1,\dots,n+1\}} A_j \right| + \sum_{i=2}^{n} \left\{ (-1)^{i+1} \sum_{\substack{S\in\{1,\dots,n+1\}^{(i)} \\ \setminus S\in\{1,\dots,n\}^{(i)}}} \left| \bigcap_{j\in S} A_j \right| \right\},$$

pa je

$$\left| \bigcup_{i=1}^{n+1} A_i \right| = \sum_{i=1}^{n+1} |A_i| + (-1)^{n+2} \left| \bigcap_{j\in\{1,\dots,n+1\}} A_j \right| + \\ + \sum_{i=2}^{n} \left\{ (-1)^{i+1} \left[\sum_{S\in\{1,\dots,n\}^{(i)}} \left| \bigcap_{j\in S} A_j \right| + \sum_{\substack{S\in\{1,\dots,n+1\}^{(i)} \\ \setminus S\in\{1,\dots,n\}^{(i)}}} \left| \bigcap_{j\in S} A_j \right| \right] \right\} = \\ = \sum_{i=1}^{n+1} |A_i| + (-1)^{n+2} \left| \bigcap_{j\in\{1,\dots,n+1\}} A_j \right| + \sum_{i=2}^{n} \left\{ (-1)^{i+1} \sum_{S\in\{1,\dots,n+1\}^{(i)}} \left| \bigcap_{j\in S} A_j \right| \right\} = \\ = \sum_{i=1}^{n+1} |A_i| + \sum_{i=2}^{n+1} \left\{ (-1)^{i+1} \sum_{S\in\{1,\dots,n+1\}^{(i)}} \left| \bigcap_{j\in S} A_j \right| \right\} = \\ = \sum_{i=1}^{n+1} \left\{ (-1)^{i+1} \sum_{S\in\{1,\dots,n+1\}^{(i)}} \left| \bigcap_{j\in S} A_j \right| \right\}.$$

□

Još jedan dokaz. Neka je $A := \bigcup_{i=1}^{n} A_i$; za $S \subseteq \{1, \ldots, n\}$ neka je $P_S := \bigcap_{i \in S} A_i$. Neka je $\mathbb{V}$ realan vektorski prostor svih funkcija ${}^A\mathbb{R}$ sa standardnom linearnom strukturom. Ako je $B \subseteq A$ neka je $\chi_B \in V := {}^A\mathbb{R}$ tzv. *karakteristična funkcija* skupa B (u odnosu na skup A), tj. funkcija data sa $\chi_B(x) = 0$ ako $x \notin A \setminus B$, $\chi_B(x) = 1$ ako $x \in B$.

Za svako $a \in A$ neka je $l_a : V \to \mathbb{R}$ funkcija definisana sa $l_a(f) = f(a)$ za svako $f \in V$; lako je videti da je l_a linearna funkcionela na $\mathbb{V}$. Zato je i $l := \sum_{a \in A} l_a$ linearna funkcionela. Neka je $J : A \to \mathbb{R}$ data sa $J(a) = 1$ za svako $a \in A$. Tvrđenje će direktno slediti ako pokažemo

$$J = \sum_{i=1}^{n} \left((-1)^{i+1} \sum_{S \in \{1,\ldots,n\}^{(i)}} \chi_{P_S} \right) \tag{II.2}$$

jer je $l(J) = \sum_{a \in A} l_a(J) = |A|$ i

$$l\left(\sum_{i=1}^{n} \left((-1)^{i+1} \sum_{S \in \{1,\ldots,n\}^{(i)}} \chi_{P_S} \right) \right) = \sum_{i=1}^{n} \left((-1)^{i+1} \sum_{S \in \{1,\ldots,n\}^{(i)}} l\left(\chi_{P_S}\right) \right) =$$

$$= \sum_{i=1}^{n} \left((-1)^{i+1} \sum_{S \in \{1,\ldots,n\}^{(i)}} |P_S| \right),$$

obzirom da je $l(\chi_B) = \sum_{a \in A} l_a(\chi_B) = |B|$ za svako $B \subseteq A$.

Dokaz jednakosti $(II.2)$ - varijanta 1: Neka je $x \in A$ proizvoljno. Neka je $\{i_1, \ldots, i_m\} = \{i \in \{1, \ldots, n\} : x \in A_i\}$, i neka je pritom $i_p \neq i_q$ za $p \neq q$. Imamo

$$\sum_{i=1}^{n} \left((-1)^{i+1} \sum_{S \in \{1,\ldots,n\}^{(i)}} \chi_{P_S} \right)(x) = \sum_{i=1}^{n} \left((-1)^{i+1} \sum_{S \in \{1,\ldots,n\}^{(i)}} \chi_{P_S}(x) \right) =$$

$$= \sum_{i=1}^{m} \left((-1)^{i+1} \sum_{S \in \{i_1,\ldots,i_m\}^{(i)}} \chi_{P_S}(x) \right) = \sum_{i=1}^{m} (-1)^{i+1} \binom{m}{i} = \binom{m}{0} - \sum_{i=0}^{m} (-1)^i \binom{m}{i} =$$

$$= \binom{m}{0} - (1-1)^m = 1\,.$$

Dokaz jednakosti $(II.2)$ - varijanta 2: Posmatrajmo (komutativni) prsten funkcija ${}^A\mathbb{Z}$ sa standardnim sabiranjem i množenjem definisanim sa $(f+g)(x) = f(x)+g(x)$ i $(f \cdot g)(x) = f(x) \cdot g(x)$. Za svako $B \subseteq A$ funkcija χ_B je jedan element dotičnog prstena; funkcija $J \in {}^A\mathbb{Z}$ je jedinica tog prstena, a funkcija $O : A \to \mathbb{Z}$ definisana sa $O(x) = 0$ za svako $x \in A$ njegova nula. Ako je $x \in A$ onda za neko $i_0 \in \{1, \ldots, n\}$ važi $x \in A_{i_0}$ pa i $\left(J - \chi_{A_{i_0}}\right)(x) = 0$. Otuda je

$$\prod_{i=1}^{n} \left(J - \chi_{A_i}\right) = O\,.$$

Odavde sada sledi

$$O = J + \sum_{i=1}^{n} \left((-1)^i \sum_{S \in \{1,\ldots,n\}^{(i)}} \prod_{j \in S} \chi_{A_j} \right)$$

što je $(II.2)$ zapisano na drugi način, obzirom da za $B_1, \ldots, B_k \subseteq A$ jasno važi $\chi_{B_1} \cdot \ldots \cdot \chi_{B_k} = \chi_{B_1 \cap \cdots \cap B_k}$.

Još jedan dokaz Neka je $A := \bigcup_{i=1}^{n} A_i = \{x_1, \ldots, x_k\}$ skup od k elemenata. Neka je $\{S_1, \ldots, S_{2^n-1}\}$ skup svih nepraznih podskupova od $\{1, \ldots, n\}$. Neka je data prazna tablica visine $2^n - 1$ a širine k. Popunimo je brojevima 1, -1 i 0 tako što u i-tu vrstu:
– ako je S_i paran broj upisujemo broj -1 u presecima sa onim kolonama za čiji redni broj j važi $x_j \in \bigcap_{l \in S_i} A_l$, odnosno broj 0 inače;
– ako je S_i neparan broj upisujemo broj 1 u presecima sa onim kolonama za čiji redni broj j važi $x_j \in \bigcap_{l \in S_i} A_l$, odnosno broj 0 inače.

Lako je videti da je suma brojeva u i-toj vrsti upravo $-\left|\bigcap_{l \in S_i} A_l\right|$ ako je S_i paran broj, odnosno $\left|\bigcap_{l \in S_i} A_l\right|$ ako je S_i neparan broj. Iz tog razloga broj na desnoj strani u (II.1) predstavlja zbir svih brojeva koji se javljaju u ovako popunjenoj tablici. S druge strane, nije teško ni videti da je zbir brojeva u svakoj koloni ponaosob uvek isti i jednak 1. Zaista, neka je $j \in \{1, \ldots, k\}$ proizvoljno, i neka je m broj elemenata

skupa $\big\{i \in \{1,\dots,n\} : x_j \in A_i\big\}$. Zbir brojeva u j-toj koloni jednak je

$$\sum_{\substack{1\le i\le m\\ i \text{ parno}}} \left(\binom{m}{i}\cdot(-1)\right) + \sum_{\substack{1\le i\le m\\ i \text{ neparno}}} \left(\binom{m}{i}\cdot 1\right) = \sum_{i=1}^{m}(-1)^{i-1}\binom{m}{i} = 1\,.$$

Tvrđenje sledi.

□

Deo III

Neke elementarne nejednakosti

III.1 Nejednakost sa permutacijama

Stav 37 Neka su dati realni brojevi $a_1 \leq a_2 \leq \cdots \leq a_n$ i $b_1 \leq b_2 \leq \cdots \leq b_n$. Neka su r_0 i r_1 permutacije skupa $\{1, \ldots, n\}$ date, redom, sa $r_0(i) = i$ i $r_1(i) = n+1-i$, tj. $r_0 = (1, 2, 3, \ldots, n-1, n)$ i $r_1 = (n, n-1, n-2, \ldots, 2, 1)$. Tada za svaku permutaciju p skupa $\{1, \ldots, n\}$ važi

$$\sum_{i=1}^{n} a_i b_{r_1(i)} \leq \sum_{i=1}^{n} a_i b_{p(i)} \leq \sum_{i=1}^{n} a_i b_{r_0(i)} .$$

Dokaz. Ako je $a_1 \leq a_2$ i $b_1 \leq b_2$ neposredno se proverava da je $a_1 b_2 + a_2 b_1 \leq a_1 b_1 + a_2 b_2$. Ovu činjenicu u nastavku koristimo bez eksplicitnog pozivanja na nju.

Za permutacije q skupa $\{1, \ldots, n\}$ neka je $S(q) :\overset{\text{df}}{=} \sum_{i=1}^{n} a_i b_{q(i)}$ i neka je, za svako $i \neq j$, $q[i, j]$ permutacija q skupa $\{1, \ldots, n\}$ data sa $q[i, j](s) = q(s)$ ako $s \notin \{i, j\}$, $q[i, j](i) = q(j)$ i $q[i, j](j) = q(i)$.

Ako je permutacija q takva da postoje $k < l$ takvi da je $q(k) > q(l)$ onda je $S(q) \leq S\left(q[k, l]\right)$. Zaista, zbog $b_{q(l)} \leq b_{q(k)}$ imamo da je

$$S(q) = \sum_{\substack{i=\overline{1,n} \\ i \notin \{i,j\}}} a_i b_{q(i)} + a_k b_{q(k)} + a_l b_{q(l)} \leq \sum_{\substack{i=\overline{1,n} \\ i \notin \{i,j\}}} a_i b_{q(i)} + a_k b_{q(l)} + a_l b_{q(k)} = S\left(q[k, l]\right) .$$

Ovo se može formulisati i ovako: ako je permutacija q takva da postoje $k < l$ takvi da je $q(k) < q(l)$ onda je $S\left(q[k, l]\right) \leq S(q)$.

Neka je sada p proizvoljna permutacija. Postoje permutacije $q_1, \ldots, q_n$ takve da je $q_i(s) = s$ za $s = \overline{1, i}$, i takve da je ili $q_1 = p$ ili $q_1 = p[k_0, l_0]$ za neke $k_0 < l_0$, kao i ili $q_{i+1} = q_i$ ili $q_{i+1} = q_i[k_i, l_i]$ za neke $k_i < l_i$. Specijalno je $q_n = r_0$. Na osnovu

prethodnog je $S(p) \leq S(q_1) \leq S(q_2) \leq \cdots \leq S(q_{n-1}) \leq S(q_n)$, pa je $S(p) \leq S(r_0)$.

Na sličan ("dualan") način se pokazuje i da važi $S(r_1) \leq S(p)$ za svaku permutaciju p.

□

III.2 Jensenova nejednakost

Primetimo da ako je $x_1, \ldots, x_n \in (p;q) \subseteq \mathbb{R}$ i $\lambda_1, \ldots, \lambda_n \geq 0$ tako da je $\sum_{i=1}^{n} \lambda_i = 1$, onda je

$$m = \sum_{i=1}^{n} \lambda_i m \leq \sum_{i=1}^{n} \lambda_i x_i \leq \sum_{i=1}^{n} \lambda_i M = M\,,$$

gde je $m = \min\{x_i : 1 \leq i \leq n\}$ i $M = \max\{x_i : 1 \leq i \leq n\}$, te je i $\sum_{i=1}^{n} \lambda_i x_i \in (p;q)$.

Definicija 7 Za funkciju $f : (p;q) \to \mathbb{R}$ kažemo da je *konveksna* [*konkavna*] na $(p;q)$ ako za svako $x, y \in (p;q)$ i svako $\lambda, \mu \geq 0$ tako da $\lambda + \mu = 1$ važi $f(\lambda x + \mu y) \leq \lambda f(x) + \mu f(y)$ $\left[\ f(\lambda x + \mu y) \geq \lambda f(x) + \mu f(y)\ \right]$.

Za funkciju $f : (p;q) \to \mathbb{R}$ kažemo da je *strogo konveksna* [*strogo konkavna*] na $(p;q)$ ako za svako $x, y \in (p;q)$ i svako $\lambda, \mu > 0$ tako da $\lambda + \mu = 1$ važi $f(\lambda x + \mu y) < \lambda f(x) + \mu f(y)$ $\left[\ f(\lambda x + \mu y) > \lambda f(x) + \mu f(y)\ \right]$ ako $x \neq y$.

□

Stav 38 Neka je $f : (p;q) \to \mathbb{R}$ diferencijabilna na $(p;q)$. Ako funkcija f' (strogo) raste na tom intervalu, onda je f (strogo) konveksna na $(p;q)$. Ako funkcija f' (strogo) opada na tom intervalu, onda je f (strogo) konkavna na $(p;q)$.

Dokaz. Pretpostavimo da je f' rastuća funkcija na $(p;q)$ (dokaz je prosto identičan i u ostalim slučajevima) i neka su $x \leq y$ iz $(p;q)$ i $\lambda, \mu \geq 0$ tako da je $\lambda + \mu = 1$. Ako je neki od brojeva $\lambda = 0$ i μ jedna nuli ili ako je $x = y$, važiće $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$. Neka je zato $x < y$ i $\lambda, \mu > 0$. Za $z := \lambda x + \mu y$ važi $x < z < y$, $\lambda = \dfrac{y-z}{y-x}$ i $\mu = \dfrac{z-x}{y-x}$. Takođe postoje $u \in (x;z)$ i $v \in (z;y)$ tako da je $\dfrac{f(z)-f(x)}{z-x} = f'(u)$ i $\dfrac{f(y)-f(z)}{y-z} = f'(v)$. Zbog $u < v$ je $f'(u) \leq f'(v)$ pa je

$$\frac{f(z)-f(x)}{z-x} \leq \frac{f(y)-f(z)}{y-z}$$

tj. $f(z) - f(x) \leq \dfrac{z-x}{y-z}\,(f(y) - f(z))$ odnosno $f(\lambda x + \mu y) \leq \lambda f(x) + \mu f(y)$.

□

Posledica 1 Neka je $f : (p;q) \to \mathbb{R}$ dva put diferencijabilna na $(p;q)$. Ako je $f''(x) \geq 0$ $[f''(x) > 0]$ za svako $x \in (p;q)$, onda je f konveksna [strogo konveksna] na $(p;q)$. Ako je $f''(x) \leq 0$ $[f''(x) < 0]$ za svako $x \in (p;q)$, onda je f konkavna [strogo konkavna] na $(p;q)$.

□

Stav 39 (*Jensenova nejednakost*) Neka je $f : (p;q) \to \mathbb{R}$ konveksna [konkavna] na $(p;q)$. Ako je $n \geq 2$, $x_1, \ldots, x_n \in (p;q)$ i $\lambda_1, \ldots, \lambda_n \geq 0$ tako da je $\sum_{i=1}^{n} \lambda_i = 1$ onda važi

$$f(\lambda_1 x_1 + \cdots + \lambda_n x_n) \leq \lambda_1 f(x_1) + \cdots + \lambda_n f(x_n)$$

$$\left[f(\lambda_1 x_1 + \cdots + \lambda_n x_n) \geq \lambda_1 f(x_1) + \cdots + \lambda_n f(x_n)\right].$$

Ako je pritom f strogo konveksna [strogo konkavna] na $(p;q)$, $\lambda_1, \ldots \lambda_n > 0$ i brojevi $x_1, \ldots, x_n$ nisu svi međusobno jednaki, onda važi i

$$f(\lambda_1 x_1 + \cdots + \lambda_n x_n) < \lambda_1 f(x_1) + \cdots + \lambda_n f(x_n)$$

$$\left[f(\lambda_1 x_1 + \cdots + \lambda_n x_n) > \lambda_1 f(x_1) + \cdots + \lambda_n f(x_n)\right].$$

Dokaz. Pretpostavimo da je f konkavna na $(p;q)$. Tvrđenje dokazujemo indukcijom po $n \geq 2$.

Ako je $n = 2$ onda je tvrđenje tačno po samoj definiciji (stroge) konkavnosti funkcija. Pretpostavimo da je tvrđenje tačno za neko $n \geq 2$ i neka su $x_1, \ldots, x_{n+1} \in (p;q)$ i $\lambda_1, \ldots, \lambda_{n+1} \geq 0$ tako da je $\sum_{i=1}^{n+1} \lambda_i = 1$. Ako je $\lambda_{n+1} = 1$ onda je $\lambda_i = 0$ za $i = \overline{1,n}$ i tvrđenje je trivijalno tačno. Zato pretpostavimo da je $\lambda_{n+1} \neq 1$. Tada je $1 - \lambda_{n+1} > 0$. Važi $\mu_i := \dfrac{\lambda_i}{1-\lambda_{n+1}} \geq 0$ za $i = \overline{1,n}$ i $\sum_{i=1}^{n} \mu_i = 1$. Imamo

$$f(\lambda_1 x_1 + \cdots + \lambda_n x_{n+1}) = f\left((1-\lambda_{n+1}) \sum_{i=1}^{n} \mu_i x_i + \lambda_{n+1} x_{n+1}\right) \overset{(1)}{\geq}$$

$$\geq (1-\lambda_{n+1}) f\left(\sum_{i=1}^{n} \mu_i x_i\right) + \lambda_{n+1} f(x_{n+1}) \overset{(2)}{\geq} (1-\lambda_{n+1}) \sum_{i=1}^{n} \mu_i f(x_i) + \lambda_{n+1} f(x_{n+1}) =$$

$$= \sum_{i=1}^{n+1} \lambda_i f(x_i)$$

gde:

– nejednakost u (1) važi zbog tačnosti baze indukcije, i pritom tu stoji stroga nejednakost " $>$ " ako važi sledeće: f je strogo konkavna, $\lambda_{n+1} \in (0;1)$ i $x_{n+1} \neq \sum_{i=1}^{n} \mu_i x_i$;

– nejednakost u (2) važi zbog indukcijske hipoteze, i pritom tu stoji stroga nejednakost " $>$ " ako važi sledeće: f je strogo konkavna, $\mu_i > 0$ za $i = \overline{1,n}$ i brojevi $x_1, \ldots, x_n$ nisu svi međusobno jednaki.

Pretpostavimo sada dodatno i to da je f strogo konkavna na $(p;q)$, da je $\lambda_1, \ldots \lambda_{n+1} > 0$ kao i da brojevi $x_1, \ldots, x_{n+1}$ nisu svi međusobno jednaki, i pokažimo da je $f(\lambda_1 x_1 + \cdots + \lambda_n x_{n+1}) > \lambda_1 f(x_1) + \cdots + \lambda_n f(x_{n+1})$. Jasno $\lambda_i \in (0;1)$ za $i = \overline{1,n+1}$.

Neka je suprotno onom što treba pokazati $f(\lambda_1 x_1 + \cdots + \lambda_n x_{n+1}) = \lambda_1 f(x_1) + \cdots + \lambda_n f(x_{n+1})$. Tada kod (1) ne stoji stroga nejednakost pa mora da je $x_{n+1} = \sum_{i=1}^{n} \mu_i x_i$. Takođe, ni kod (2) ne stoji stroga nejednakost pa mora da je $x_i = x_j$ za $i, j \in \{1, \ldots, n\}$. Zaključujemo da je $x_{n+1} = \left(\sum_{i=1}^{n} \mu_i \right) x_1 = x_1$, te je $x_i = x_j$ za $i, j \in \{1, \ldots, n+1\}$, suprotno pretpostavci.

Tvrđenje za slučaj da je f (strogo) konveksna se dokazuje analogno.

□

Stav 40 (*Uopštena* AG *nejednakost*) Neka je $n \geq 2$, $x_1, \ldots, x_n > 0$ i $\lambda_1, \ldots, \lambda_n \geq 0$ tako da je $\sum_{i=1}^{n} \lambda_i = 1$. Tada je

$$\lambda_1 x_1 + \cdots + \lambda_n x_n \geq x_1^{\lambda_1} \cdot \ldots \cdot x_n^{\lambda_n}.$$

Ako je $\lambda_1, \ldots, \lambda_n > 0$, onda gore važi jednakost akko su brojevi $x_1, \ldots, x_n$ svi međusobno jednaki.

Dokaz. Funkcija $\ln : (0;+\infty) \to \mathbb{R}$ je dva put diferencijabilna i $(\ln')(x) = -\dfrac{1}{x^2} < 0$ za svako $x \in (0;+\infty)$. Dakle ln je strogo konkavna na $(0;+\infty)$ te važi

$$\ln(\lambda_1 x_1 + \cdots + \lambda_n x_n) \geq \lambda_1 \ln(x_1) + \cdots + \lambda_n \ln(x_n),$$

i pritom ako je $\lambda_1, \ldots, \lambda_n > 0$, onda ovde važi stroga nejednakost čim brojevi $x_1, \ldots, x_n$ nisu svi međusobno jednaki. Funkcija $h : \mathbb{R} \to (0;+\infty)$ data sa $h(x) = \mathrm{e}^x$ je stogo rastuća funkcija, pa dalje sledi da je

$$\mathrm{e}^{\ln(\lambda_1 x_1 + \cdots + \lambda_n x_n)} \geq \mathrm{e}^{\lambda_1 \ln(x_1) + \cdots + \lambda_n \ln(x_n)},$$

i pritom ako je $\lambda_1, \ldots, \lambda_n > 0$, onda ovde važi stroga nejednakost čim brojevi $x_1, \ldots, x_n$ nisu svi međusobno jednaki. Dakle $\lambda_1 x_1 + \cdots + \lambda_n x_n \geq x_1^{\lambda_1} \cdot \ldots \cdot x_n^{\lambda_n}$, i pritom ako je $\lambda_1, \ldots, \lambda_n > 0$, onda ovde važi stroga nejednakost čim brojevi $x_1, \ldots, x_n$ nisu svi međusobno jednaki.

□

III.3 Nejednakosti između klasičnih sredina

Ako je $n \in \mathbb{N}$ i $\overrightarrow{x} = (x_1, \ldots, x_n) \in [0; +\infty)^n$ onda definišemo

Aritmetičku sredinu n-torke $\overrightarrow{x}$: $\mathrm{A}_n(\overrightarrow{x}) :\overset{\mathrm{df}}{=} \dfrac{1}{n}\sum_{i=1}^{n} x_i$;

Geometrijsku sredinu n-torke $\overrightarrow{x}$: $\mathrm{G}_n(\overrightarrow{x}) :\overset{\mathrm{df}}{=} \left\{\prod_{i=1}^{n} x_i\right\}^{\frac{1}{n}}$;

Kvadratnu sredinu n-torke $\overrightarrow{x}$: $\mathrm{K}_n(\overrightarrow{x}) :\overset{\mathrm{df}}{=} \sqrt{\dfrac{1}{n}\sum_{i=1}^{n}(x_i)^2}$;

i, pod uslovom da je $x_i > 0$ za svako $i = \overline{1,n}$, i

Harmonijsku sredinu n-torke $\overrightarrow{x}$: $\mathrm{H}_n(\overrightarrow{x}) :\overset{\mathrm{df}}{=} \dfrac{n}{\sum_{i=1}^{n}\dfrac{1}{x_i}}$.

Takođe, "$u \leq_{\overrightarrow{x}} v$" će značiti:

"$u \leq v$ i jednakost $u = v$ važi jedino ako je $x_i = x_j$ za sve $1 \leq i, j \leq n$".

Stav 41 (AG *nejednakost*) Za svako $n \in \mathbb{N}$ i svako $\overrightarrow{x} \in [0; +\infty)^n$ važi

$$\mathrm{G}_n(\overrightarrow{x}) \leq_{\overrightarrow{x}} \mathrm{A}_n(\overrightarrow{x})\,.$$

Dokaz. Ako je $x_i = 0$ za neko $i \in \{1, \ldots, n\}$ onda tvrđenje sledi trivijalno, a ako je $x_i > 0$ za svako $i = \overline{1,n}$, onda je tvrđenje specijalan slučaj Tvrđenja 40.

U nastavku dajemo jedan drugi dokaz ovog tvrđenja koji ne koristi pojam diferencijabilnosti funkcija (koji je korišćen za dokaz Tvrđenja 40).

Za svako $k \in \mathbb{N}$ označimo sa T_k iskaz:

"za svako $\overrightarrow{x} \in [0; +\infty)^k$ važi $\mathrm{G}_k(\overrightarrow{x}) \leq_{\overrightarrow{x}} \mathrm{A}_k(\overrightarrow{x})$".

(A) Pokazujemo da je T_2 tačno. Ako su $x_1, x_2 \geq 0$ imamo

$$\sqrt{x_1x_2} \leq \frac{x_1+x_2}{2} \iff 0 \leq (\sqrt{x_1})^2 + (\sqrt{x_2})^2 - 2\sqrt{x_1}\sqrt{x_2} \iff 0 \leq (\sqrt{x_1} - \sqrt{x_1})^2$$

odakle se vidi da je T_2 je tačno $\big($obzirom da je $\sqrt{x_1x_2} = \dfrac{x_1+x_2}{2} \iff 0 = (\sqrt{x_1} - \sqrt{x_1})^2\big)$.

(B) Pokazujemo $\mathrm{T}_k \Rightarrow \mathrm{T}_{2k}$. Neka važi T_k i neka je $\overrightarrow{x} \in [0;+\infty)^{2k}$ proizvoljno. Imamo, za $a := \dfrac{1}{k}\displaystyle\sum_{i=1}^{k} x_i$ i $b := \dfrac{1}{k}\displaystyle\sum_{i=k+1}^{2k} x_i$,

$$\prod_{i=1}^{k} x_i \prod_{i=k+1}^{2k} x_i \overset{(1)}{\leq} \left(\frac{\displaystyle\sum_{i=1}^{k} x_i}{k}\right)^k \left(\frac{\displaystyle\sum_{i=k+1}^{2k} x_i}{k}\right)^k \underset{(a,b)}{\overset{(2)}{\leq}} \left[\left(\frac{\displaystyle\sum_{i=1}^{k} x_i + \sum_{i=k+1}^{2k} x_i}{2k}\right)^2\right]^k =$$

$$= \left(\frac{1}{2k}\sum_{i=1}^{2k} x_i\right)^{2k}$$

gde "$\leq$" na mestu (1) stoji na osnovu T_k. Ovim je pokazano da važi $\mathrm{G}_{2k}(\overrightarrow{x}) \leq \mathrm{A}_{2k}(\overrightarrow{x})$.

Pretpostavimo sada da je $\mathrm{G}_{2k}(\overrightarrow{x}) = \mathrm{A}_{2k}(\overrightarrow{x})$. Tada mestu (2) stoji "=" pa je $a = b$. Kako i na mestu (1) stoji "=" to mora biti:

Slučaj 1: ako $x_{i_0} = 0$ za neko $1 \leq i_0 \leq 2k$ onda iz $\displaystyle\sum_{i=1}^{2k} x_i = 0$, a kako je $x_i \geq 0$ za svako $1 \leq i \leq 2k$, sledi da je $x_i = 0$ za svako $1 \leq i \leq 2k$;

Slučaj 2: ako $x_i > 0$ za svako $1 \leq i \leq 2k$ onda zbog T_k $\big($a na osnovu jednostavne činjenice da $(r < s \wedge p \leq q \neq 0) \Rightarrow rp < sq)\big)$ zaključujemo da je $\displaystyle\prod_{i=1}^{k} x_i = \left(\frac{1}{k}\sum_{i=1}^{k} x_i\right)^k$ i $\displaystyle\prod_{i=k+1}^{2k} x_i = \left(\frac{1}{k}\sum_{i=k+1}^{2k} x_i\right)^k$; sada na osnovu T_k dobijamo $x_i = x_j$ za sve $1 \leq i, j \leq k$ kao i $x_i = x_j$ za sve $k+1 \leq i, j \leq 2k$, pa je i $x_i = a = b = x_j$ za $1 \leq i \leq k$ i $k+1 \leq j \leq 2k$; dakle $\overrightarrow{x}$ je konstantna $2k$-torka.

(C) Pokazujemo T_n za proizvoljno $n \geq 2$. Najpre primetimo da se iz (A) i (B) induktivnim rezonovanjem može zaključiti da je T_{2^k} tačno za svako $k \in \mathbb{N}$.

Neka je $\overrightarrow{x} \in [0;+\infty)^n$ i neka je $k \in \mathbb{N}$ takvo da je $2^k > n$. Definišimo $\overrightarrow{y} = (y_1, \ldots, y_{2^k}) \in [0;+\infty)^{2^k}$ sa $y_i = x_i$ za $1 \leq i \leq n$, i $y_i = \mathrm{A}_n(\overrightarrow{x}) =: \alpha$ za $n < i \leq 2^k$.

Stavimo $m := 2^k - n$. Kako važi T_{2^k} to je $\mathrm{G}_{2^k}(\overrightarrow{y}) \leq \mathrm{A}_{2^k}(\overrightarrow{y})$ pa je

$$\prod_{i=1}^{n} x_i \cdot \alpha^m \leq \left(\frac{\sum_{i=1}^{n} x_i + m\alpha}{2^k} \right)^{2^k} = \left(\frac{n+m}{2^k}\alpha \right)^{2^k} = \alpha^{2^k} \quad \dots (*)$$

Ako je $\alpha = 0$ onda je $x_i = 0$ za svako $1 \leq i \leq n$ te važi $\mathrm{G}_n(\overrightarrow{x}) \leq \mathrm{A}_n(\overrightarrow{x})$.
Ako je $\alpha > 0$ onda iz $(*)$ sledi $\prod_{i=1}^{n} x_i \leq \alpha^n$, tj. $\mathrm{G}_n(\overrightarrow{x}) \leq \mathrm{A}_n(\overrightarrow{x})$.
Dakle nejednakost $\mathrm{G}_n(\overrightarrow{x}) \leq \mathrm{A}_n(\overrightarrow{x})$ je dokazana.

Pretpostavimo sada da je $\mathrm{G}_n(\overrightarrow{x}) = \mathrm{A}_n(\overrightarrow{x})$, tj. $\prod_{i=1}^{n} x_i \leq \alpha^n$. Množenjem ove jednakosti sa α^m odavde sledi

$$\prod_{i=1}^{n} x_i \cdot \alpha^m = \left(\frac{\sum_{i=1}^{n} x_i + m\alpha}{2^k} \right)^{2^k}$$

tj. $\mathrm{G}_{2^k}(\overrightarrow{y}) = \mathrm{A}_{2^k}(\overrightarrow{y})$, pa obzirom na to da važi T_{2^k} zaključujemo da mora biti $x_i = y_i = y_j = x_j$ za sve $1 \leq i, j \leq n$. □

Stav 42 (AK *nejednakost*) Za svako $n \in \mathbb{N}$ i svako $\overrightarrow{x} \in [0; +\infty)^n$ važi

$$\mathrm{A}_n(\overrightarrow{x}) \leq_{\overrightarrow{x}} \mathrm{K}_n(\overrightarrow{x})\,.$$

Dokaz. Za $a, b \in \mathbb{R}$ imamo $2ab \leq a^2 + b^2$ i pritom je $2ab < a^2 + b^2$ ako $a \neq b$. U nastavku ovo koristimo bez eksplicitnog naglašavanja.

Imamo

$$(x_1 + \cdots + x_n)^2 = \sum_{i=1}^{n} x_i^2 + \sum_{1 \leq i < j \leq n} 2x_i x_j \overset{(1)}{\leq} \sum_{i=1}^{n} x_i^2 + \sum_{1 \leq i < j \leq n} (x_i^2 + x_j^2) = n \sum_{i=1}^{n} x_i^2\,,$$

pri čemu kod (1) stoji stroga nejednakost čim važi $x_i \neq x_j$ za neko $i \neq j$.

□

Stav 43 (AH *nejednakost*) Za svako $n \in \mathbb{N}$ i svako $\overrightarrow{x} \in (0; +\infty)^n$ važi

$$\mathrm{H}_n(\overrightarrow{x}) \leq_{\overrightarrow{x}} \mathrm{G}_n(\overrightarrow{x})\,.$$

Dokaz. Imamo

$$\mathrm{H}_n(\overrightarrow{x}) \leq_{\overrightarrow{x}} \mathrm{G}_n(\overrightarrow{x})$$

akko

$$\mathrm{A}_n((1/x_1, \dots, 1/x_n)) \geq_{\overrightarrow{x}} \mathrm{G}_n((1/x_1, \dots, 1/x_n))\,.$$

□

Deo IV

Diferencne jednačine

IV.1 Linearna homogena diferencna jednačina sa konstantnim koeficijentima

Neka su dati $n \in \mathbb{N}$ i $c_0, c_1, \ldots, c_{n-1} \in \mathbb{C}$.

Linearna homogena diferencna jednačina n-tog reda sa n-torkom koeficijenata $(c_0, c_1, \ldots, c_{n-1})$ je diferencna jednačina

$$a_{k+n} = c_{n-1}a_{k+n-1} + \cdots + c_1 a_{k+1} + c_0 a_k \qquad (*)$$

gde je $c_0 \neq 0$, a njeno rešenje je svaki niz $\langle a_k |\ k \in \mathbb{N}\rangle$ kompleksnih brojeva za koji $(*)$ važi za svako $k \in \mathbb{N}$.

Polinom $q(x) := x^n - c_{n-1}x^{n-1} - \cdots - c_1 x - c_0$ naziva se *karakteristični polinom diferencne jednačine* $(*)$. Primetimo da je $q(0) \neq 0$.

Neka je $\mathbb{V}$ vektorski prostor svih nizova kompleksnih brojeva sa uobičajenim sabiranjem nizova i množenjem kompleksnim brojem. k-ti element nekog niza a označavaćemo podjednako i sa a_k i sa $a(k)$.

Neka je definisano preslikavanje $L : \mathbb{V} \to \mathbb{V}$ sa $L(a) = b$ akko $\forall k \in \mathbb{N}\ (b_k = a_{k+1})$. Jasno, ako je i nenegativan ceo broj, $L^i(a) = b$ akko $b_k = a_{k+i}$ za svako $k \in \mathbb{N}$. Jednostavno je videti da je L linearno preslikavanje.

Zadatak. Za prirodne brojeve $s \geq 1$ i p gde $0 \leq p \leq s-1$ označimo $f(s,p) = \sum_{i=0}^{s} \binom{s}{i} (-1)^i\ i^p$. Dokazati da je uvek $f(s,p) = 0$.

Rešenje. Indukcijom po $s \geq 1$ pokazujemo da važi

$$0 \leq p \leq s-1 \ \Rightarrow\ f(s,p) = 0.$$

Za $s = 1$ direktnom proverom se utvrđuje tačnost tvrđenja.

Neka je $f(s,p) = 0$ za neko $s \geq 1$ i svako p gde $0 \leq p \leq s-1$.
Pokažimo najpre $f(s+1,p) = 0$ za $p = 0$.
$f(s+1,0) = \sum_{i=0}^{s+1} \binom{s+1}{i}(-1)^i = (1-1)^{s+1} = 0.$
Neka je sada $1 \leq p \leq s$.

$$f(s+1,p) =$$

$$\sum_{i=0}^{s+1} \binom{s+1}{i}(-1)^i\ i^p =$$

$$\binom{s+1}{0}(-1)^0 \cdot 0^p + (s+1)\ \sum_{i=1}^{s+1} \binom{s}{i-1}(-1)^i\ i^{p-1} =$$

$$0 + (s+1)\ \sum_{m=0}^{s} \binom{s}{m}(-1)^{m+1}(m+1)^{p-1} =$$

$$-(s+1)\sum_{m=0}^{s} \binom{s}{m}(-1)^m\ \sum_{r=0}^{p-1} \binom{p-1}{r} m^r =$$

$$-(s+1)\sum_{r=0}^{p-1} \binom{p-1}{r} \sum_{m=0}^{s} \binom{s}{m}(-1)^m m^r =$$

$$-(s+1)\sum_{r=0}^{p-1} \binom{p-1}{r} f(s,r) = 0$$

po indukcijskoj hipotezi jer je $0 \leq r \leq p-1 \leq s-1$. $\square$

Stav 44 Neka je $R \in \mathbb{C}$ koren višestrukosti l karakterističnog polinoma $q(x)$ jednačine $(*)$, gde $1 \leq l \leq n$.

Ako je $0 \leq s < l$ onda je niz $\langle k^s R^k |\ k \in \mathbb{N}\rangle$ rešenje jednačine $(*)$.

Dokaz. Kako je višestrukost nule R polinoma $q(x)$ jednaka $l > s$ to je $q(x) = (x-R)^{s+1} \cdot g(x)$ za neki polinom g stepena $n-s-1$.

Primetimo da je

$$a_{k+n} - c_{n-1}a_{k+n-1} - \cdots - c_1 a_{k+1} - c_0 a_k =$$

$$L^n(a)(k) - c_{n-1}L^{n-1}(a)(k) - \cdots - c_1 L^1(a)(k) - c_0 L^0(a)(k) =$$

$$(L^n(a) - c_{n-1}L^{n-1}(a) - \cdots - c_1L^1(a) - c_0L^0(a))(k) =$$

$$= (q(L)(a))(k)$$

pa zapravo treba pokazati da je za svako $k \in \mathbb{N}$ $(q(L)(a))(k) = 0$. Neka je $I = L^0$ identičko preslikavanje prostora $\mathbb{V}$.

$q(L)(a) = [(L - R \cdot I)^{s+1} \circ g(L)](a) = [g(L) \circ (L - R \cdot I)^{s+1}](a) = g(L)((L - R \cdot I)^{s+1}(a))$ pa je dovoljno, budući da je $g(L)$ linearno preslikavanje, pokazati da je $z := (L - R \cdot I)^{s+1}(a)$ konstantan nula niz, tj. $z_k = 0$ za svako $k \in \mathbb{N}$. Imamo

$$z_k = [\ \sum_{i=0}^{s+1} \binom{s+1}{i} (-1)^{s+1-i} R^{s+1-i} \cdot L^i(a)](k) =$$

$$\sum_{i=0}^{s+1} \binom{s+1}{i} (-1)^{s+1-i} R^{s+1-i} a_{k+i} =$$

$$\sum_{i=0}^{s+1} \binom{s+1}{i} (-1)^{s+1-i} R^{s+1-i} (k+i)^s R^{k+i} =$$

$$R^{s+1+k}(-1)^{s+1} \sum_{i=0}^{s+1} \binom{s+1}{i} (-1)^i \sum_{j=0}^{s} \binom{s}{j} k^j i^{s-j} =$$

$$R^{s+1+k}(-1)^{s+1} \sum_{j=0}^{s} \binom{s}{j} k^j \sum_{i=0}^{s+1} \binom{s+1}{i} (-1)^i i^{s-j} =$$

$$R^{s+1+k}(-1)^{s+1} \sum_{j=0}^{s} \binom{s}{j} k^j f(s+1, s-j) = 0$$

gde $f(s+1, s-j)$ označava istu sumu kao i u prethodnom zadatku, a za koju znamo da je jednaka nuli na osnovu istog jer je $0 \leq s - j \leq s$. $\square$

Skup $\Lambda := \{a \in \mathbb{V} |\ a$ je rešenje jednačine $(*)\}$ je podprostor od $\mathbb{V}$, što se lako uočava.

Preslikavanje $CUT : \Lambda \to \mathbb{C}^n$ definisano sa $CUT(a) := (a_1, \ldots, a_n)$ je linearno i bijektivno te je izomorfizam prostora Λ i $\mathbb{C}^n$. Imamo, specijalno, da je $dim\Lambda = n$.

Neka je $R \in \mathbb{C}$ koren višestrukosti l karakterističnog polinoma $q(x)$ jednačine $(*)$, gde $1 \leq l \leq n$.

Pokažimo da su vektori $\langle k^s R^k |\ k \in \mathbb{N} \rangle,\ 0 \leq s < l$, prostora Λ linearno nezavisni. Ekvivalentno, pokažimo da su njihove slike preslikavanjem CUT linearno nezavisni vektori prostora $\mathbb{C}^n$.

Kako je

$$\begin{vmatrix} R & 1\cdot R & \dots & 1^{l-1}\cdot R \\ R^2 & 2\cdot R^2 & \dots & 2^{l-1}\cdot R^2 \\ \vdots & \vdots & \dots & \vdots \\ R^l & l\cdot R^l & \dots & l^{l-1}\cdot R^l \end{vmatrix} =$$

$$R^{\frac{l(l+1)}{2}} \cdot \begin{vmatrix} 1 & 1 & \dots & 1^{l-1} \\ 1 & 2 & \dots & 2^{l-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & l & \dots & l^{l-1} \end{vmatrix} =$$

$$R^{\frac{l(l+1)}{2}} \cdot W(1,2,3,\dots,l) \neq 0$$

(gde $W(x_1,\dots,x_l)$ označava determinantu *Vandermonde*-ove matrice koja odgovara l-torci brojeva $(x_1,\dots,x_l)$) to je rang matrice

$$\begin{bmatrix} R & 1\cdot R & \dots & 1^{l-1}\cdot R \\ R^2 & 2\cdot R^2 & \dots & 2^{l-1}\cdot R^2 \\ \vdots & \vdots & \dots & \vdots \\ R^n & n\cdot R^n & \dots & n^{l-1}\cdot R^n \end{bmatrix}$$

jednak l, te su "*kolone*" ove matrice linearno nezavisni vektori prostora $\mathbb{C}^n$.

Neka je sada $q(x) = \prod_{i=1}^{h} (x-R_i)^{l_i}$, gde je $R_i \neq R_j$ za $i \neq j$. Jasno $l_1+\dots+l_h = n$.

Za $1 \leq i \leq h$ i $0 \leq j < l_i$ označimo $u_{i,j} := \langle k^j R_i^k |\ k \in \mathbb{N}\rangle$ i pokažimo da je sistem rešenja $\langle u(i,j)|\ 1 \leq i \leq h,\ 0 \leq j < l_i\rangle$ linearno nezavisan sistem vektora prostora Λ. Ako uvedemo oznake $Q_i := \mathcal{L}(u_{i,j}|0 \leq j < l_i)$, za $1 \leq i \leq h$, za to je dovoljno, obzirom na upravo utvrđenu linearnu nezavisnost u prethodnoj analizi, pokazati da je suma $Q_1 + \dots + Q_h$ direktna. Kako je CUT izomorfizam, ova suma je direktna ako i samo ako je suma $P_1 + \dots + P_h$ direktna, gde je

$$P_i := \{\mathrm{CUT}(x)\ :\ x \in Q_i\} \subseteq \mathbb{C}^n$$

za $i = \overline{1,h}$. Da je suma $P_1 + \dots + P_h$ direktna slediće iz naredne dve leme.

Lema 1 Preslikavanje $A : \mathbb{C}^n \to \mathbb{C}^n$ definisano sa

$$A((x_1,\dots,x_{n-1},x_n)) := (x_2, x_3, \dots, x_n,\ \sum_{m=0}^{n-1} c_m x_{m+1})$$

je linearno. Ako je α koren višestrukosti p karakterističnog polinoma q, i ako je $b_i := \langle k^i \alpha^k |\ k \in \mathbb{N}\rangle$ za $0 \leq i < p$, tada je $P := \{\mathrm{CUT}(x) : x \in \mathcal{L}(b_0,\dots,b_{p-1})\}$ A-invarijantan podprostor od $\mathbb{C}^n$, i pritom je jedina sopstvena vrednost restrikcije operatora A na podprostor P upravo broj α.

Dokaz. Da je preslikavanje A linearno je očigledno. Ako stavimo $v_i := \mathrm{CUT}(b_i)$, za $0 \leq i < p$, imamo da je sistem $v = (v_0, \ldots, v_{p-1})$ je baza za P (jer je CUT linearni izomorfizam). Preslikajmo vektore sistema v preslikavanjem A:

$$A(v(i)) = A\left((1^i\alpha^1,\ 2^i\alpha^2, \ldots, n^i\alpha^n)\right) =$$

$$\left(2^i\alpha^2, 3^i\alpha^3, \ldots, n^i\alpha^n,\ \sum_{m=0}^{n-1} c_m(m+1)^i\alpha^{m+1}\right) =$$

$$\left(2^i\alpha^2, 3^i\alpha^3, \ldots, n^i\alpha^n, (n+1)^i\alpha^{n+1}\right) =$$

$$\alpha\cdot\left((1+1)^i\alpha^1,\ (2+1)^i\alpha^2, \ldots, ((n-1)+1)^i\alpha^{n-1}, (n+1)^i\alpha^n\right) =$$

$$\alpha\cdot\left(\sum_{m=0}^{i}\binom{i}{m}1^m\alpha^1,\ \sum_{m=0}^{i}\binom{i}{m}2^m\alpha^2, \ldots,\ \sum_{m=0}^{i}\binom{i}{m}(n-1)^m\alpha^{n-1},\ \sum_{m=0}^{i}\binom{i}{m}n^m\alpha^n\right)$$

$$= \sum_{m=0}^{i}\alpha\binom{i}{m}\cdot(1^m\alpha^1,\ 2^m\alpha^2, \ldots, n^m\alpha^n)$$

$$= \sum_{m=0}^{i}\alpha\binom{i}{m}v_m.$$

Iz ovog zaključujemo da je $A(v_i) \in P$ za svako $0 \leq i < p$, te da je $A[P] \subseteq P$. Zato je restrikcija, u oznaci A_1, operatora A na podprostor P endomorfizam prostora P. Iz prethodnog se takođe vidi da je matrica operatora A_1 u odnosu na bazu v gornja trougaona pri čemu su joj vrednosti na glavnoj dijagonali uvek jednake α. Zato je karakteristični polinom operatora A_1 polinom $(x-\alpha)^p$ pa je jedina sopstvena vrednost operatora A_1 broj α. $\square$

Lema 2 Neka je $A : V \to V$ endomorfizam konačnodimenzionalnog vektorskog prostora $\mathbb{V}$. Ako je $k \in \mathbb{N}$ ako su $Q_1, \ldots, Q_k \subseteq V$ A-invarijantni podprostori od $\mathbb{V}$ takvi da, kakvi god da su $1 \leq i < j \leq k$, ne postoji zajednička sopstvena vrednost restrikcija $A_i := A \restriction Q_i$ i $A_j := A \restriction Q_j$, onda je suma $Q_1 + \cdots + Q_k$ direktna.

Dokaz Indukcijom po $k \in \mathbb{N}$. Neka je najpre $k = 2$. Pokazujemo da je $Q_1 \cap Q_2 = \{\mathbf{0}\}$. Pretpostavimo suprotno, tj. neka je $Q_1 \cap Q_2$ pozitivne dimenzije. Kako su i Q_1 i Q_2 A-invarijantni podprostori, to je takav i $Q_1 \cap Q_2$. Ako stavimo $A_0 := A \restriction (Q_1 \cap Q_2)$, onda je A_0 endomorfizam konačnodimenzionalnog nenula vektorskog prostora $Q_1 \cap Q_2$ pa postoji neko $\lambda \in \mathbb{C}$ koje je sopstvena vrednost operatora A_0. No tada je λ sopstvena vrednost i operatora A_1 i operatora A_2, suprotno pretpostavci.

Pretpostavimo sada da je trđenje tačno za svako $k < m$ i neka su $Q_1, \ldots, Q_m \subseteq V$ A-invarijantni podprostori od $\mathbb{V}$ takvi da, kakvi god da su $1 \leq i < j \leq m$, ne postoji zajednička sopstvena vrednost restrikcija A_i i A_j. Neka je $i_0 \in \{1, \ldots, m\}$

proizvoljno i stavimo $(Q_1, \ldots, Q_{i_0-1}, Q_{i_0+1}, \ldots, Q_m, Q_{i_0}) = (P_1, \ldots, P_m)$. Treba pokazati da je

$$M := P_m \cap \sum_{1 \le j < m} P_j = \{\mathbf{0}\}$$

Kako presek A-invarijantnih podprostora i sam M je A-invarijantan podprostor. Označimo sa A_0 restrikciju $A \restriction M \in \mathrm{End}(M)$. Ako pretpostavimo da M nije nula podprostor, tj. da je dimenzije bar 1, onda postoji bar jedna sopstvena vrednost $\lambda \in \mathbb{C}$ operatora A_0. Dakle za neki $z \in M \setminus \{\mathbf{0}\}$ važi $A(z) = \lambda z$.

Imamo $P_m \ni z = p_1 + \cdots + p_{m-1}$, za neke $p_i \in P_i$, $i = \overline{1, m-1}$. Otuda je

$$\lambda p_1 + \cdots + \lambda p_{m-1} = \lambda z = A(z) = A(p_1) + \cdots + A(p_{m-1})$$

Suma $P_1 + \cdots + P_{m-1}$ je direktna, prema indukcijskoj hipotezi, i važi $A(p_i) \in P_i$ za svako $i = \overline{1, m-1}$, pa sledi da mora biti

$$A(p_i) = \lambda p_i \quad \text{za svako} \quad i = \overline{1, m-1}$$

Postoji neko $i_0 \in \{1, \ldots, m-1\}$ tako da je $p_{i_0} \neq \mathbf{0}$ (u suprotnom bi bilo $z = \mathbf{0}$). Tada je λ sopstvena vrednost za operator A_{i_0}. No, zbog $\mathbf{0} \neq z \in M \subseteq P_m$, λ je sopstvena vrednost i za operator A_m – kontradikcija. $\square$

Kao što smo ranije zapazili, iz ove leme sada sledi da nizovi $\langle u(i,j) |\ 1 \le i \le h,\ 0 \le j < l_i \rangle$ čine linearno nezavisan sistem vektora prostora Λ, te kako je dužina ovog sistema jednaka $l_1 + \cdots + l_h = n = \dim\Lambda$ ovaj sistem je zapravo baza ovog prostora. Zato je svako rešenje jednačine $(*)$, tj. svaki vektor iz Λ linearna kombinacija vektora te baze. Ukratko važi sledeća teorema.

Teorema 5 Niz a je rešenje jednačine $(*)$ akko za svako i, gde $1 \le i \le h$, postoji polinom $z_i(x)$ stepena ne većeg od $l_i - 1$, tako da važi

$$a_k = z_1(k) R_1^k + \cdots + z_h(k) R_h^k. \quad \square$$

Deo V

Neke teme o polinomima

V.1 Šturmov algoritam

Neka je dat polinom q sa realnim koeficijentima. Niz $\langle p_i | 0 \leq i \leq k \rangle$, $k \geq 1$, polinoma sa realnim koeficijentima se naziva *Šturmov niz* za polinom q ako je $p_0 = q$ i ako važi:
(i) p_k nema realnih korena;
(ii) p_i i p_{i+1} nemaju zajedničkih korena ni za jedno $0 \leq i < k$;
(iii) ako je $p_i(\alpha) = 0$ za neko $1 \leq i < k$ i neko $\alpha \in \mathbb{R}$ onda je $p_{i-1}(\alpha)p_{i+1}(\alpha) < 0$;
(iv) ako je $q(\alpha) = 0$ za neko $\alpha \in \mathbb{R}$ onda postoji $\epsilon > 0$ tako da je $q(x)p_1(x) < 0$ za svako $x \in (\alpha - \epsilon, \alpha)$ i $q(x)p_1(x) > 0$ za svako $x \in (\alpha, \alpha + \epsilon)$.

Neka je $\langle p_i | 0 \leq i \leq k \rangle$, $k \geq 1$, konačan niz polinoma sa realnim koeficijentima. Ako je $x_0 \in \mathbb{R}$ onda ćemo za $i \in I := \{0, \ldots, k\}$ reći da je *indeks promene u tački x_0 u odnosu na dati niz* ako postoji neko $j \in I$, $j > i$, tako da je
- $p_i(x_0)p_j(x_0) < 0$ i
- ako je $s \in I$ takvo da $i < s < j$ onda mora biti $p_s(x_0) = 0$.

Neka jednostavna zapažanja koja treba upamtiti: Primetimo da iz same definicije sledi da k nikad **nije** indeks promene u tački x_0, kao i da ako je $i \in I$ takvo da $p_i(x_0) = 0$ onda i **nije** indeks promene u tački x_0. Takođe, ako je $0 \leq i < k$ takvo da je $p_i(x_0) \neq 0$ i $p_{i+1}(x_0) \neq 0$ onda važi: i je indeks promene u tački x_0 **akko** $p_i(x_0)p_{i+1}(x_0) < 0$.

Sa $S(x_0)$ ćemo označavati skup svih indekasa promene u tački x_0, tj. $S(x_0) :\overset{\text{df}}{=} \{i \in I |\ i \text{ je indeks promene u tački } x_0\}$. *Funkcija promena znaka* u datom nizu je funkcija $W : \mathbb{R} \to \mathbb{R}$ definisana sa $W(x) = \text{card}\big(S(x)\big)$ (tj. $W(x)$ je broj indekasa promene u tački x) za $x \in \mathbb{R}$.

Primer. Neka je $p_0(x) = x - 1$, $p_1(x) = x + 1$, $p_2(x) = x^2 - 1$, $p_3(x) = (x-1)^2$, $p_4(x) = x + 2$, $p_5(x) = x^3 - 1$, $p_6(x) = x^2 - 3x + 2$, $p_7(x) = -x$ i $p_8(x) = x^2$. Tada je

$$\begin{bmatrix} \operatorname{sgn}\big(p_0(1)\big) \\ \operatorname{sgn}\big(p_1(1)\big) \\ \operatorname{sgn}\big(p_2(1)\big) \\ \operatorname{sgn}\big(p_3(1)\big) \\ \operatorname{sgn}\big(p_4(1)\big) \\ \operatorname{sgn}\big(p_5(1)\big) \\ \operatorname{sgn}\big(p_6(1)\big) \\ \operatorname{sgn}\big(p_7(1)\big) \\ \operatorname{sgn}\big(p_8(1)\big) \end{bmatrix} = \begin{bmatrix} 0 \\ +1 \\ 0 \\ 0 \\ +1 \\ 0 \\ 0 \\ -1 \\ +1 \end{bmatrix}$$

pa je $S(1) = \{4, 7\}$ i $W(1) = 2$. $\square$

Teorema 6 Ako je q polinom sa realnim koeficijentima, $\langle p_i | 0 \le i \le k \rangle$, $k \ge 1$, neki njegov Šturmov niz i $a, b \in \mathbb{R}$ onda je broj realnih korena polinoma q koje se nalaze u poluzatvorenom intervalu $(a, b]$ upravo $W(a) - W(b)$, gde je W funkcija promena znaka u tom Šturmovom nizu.

Dokaz. Neka je $I := \{0, 1, \ldots, k\}$ i $N := \{x \in \mathbb{R} | \exists i \in I(p_i(x) = 0)\}$. N je konačan skup.
Pomoćno tvrđenje 1. Neka su $u, v \in \mathbb{R}$, $u < v$ takvi da je $N \cap (u, v) = \emptyset$, i neka su $t_1, t_2 \in (u, v)$. Tada za svako $i \in I$ važi $\operatorname{sgn}\big(p_i(t_1)\big) = \operatorname{sgn}\big(p_i(t_2)\big) \neq 0$ (gde je $\operatorname{sgn}(0) = 0$, $\operatorname{sgn}(x) = 1$ ako $x > 0$ i $\operatorname{sgn}(x) = -1$ ako $x < 0$). Takođe je $S(t_1) = S(t_2)$ kao i $W(t_1) = W(t_2)$.
Dokaz. Neka je $i \in I$. Kako je $(u, v) \cap N = \emptyset$ to za svako $x \in (u, v)$ važi $p_i(x) \neq 0$. Specijalno sledi $\operatorname{sgn}\big(p_i(t_j)\big) \in \{-1, 1\}$ za $j = \overline{1, 2}$. Kad bi bilo $\operatorname{sgn}\big(p_i(t_1)\big) \cdot \operatorname{sgn}\big(p_i(t_2)\big) < 0$ onda bi (zbog neprekidnosti funkcije p_i) za neko $t_1 < w < t_2$ moralo biti $p_i(w) = 0$; no znamo da je $p_i(x) \neq 0$ za svako $x \in (u, v)$. Dakle $\operatorname{sgn}\big(p_i(t_1)\big) = \operatorname{sgn}\big(p_i(t_2)\big) \neq 0$.

Imamo da je $i \in S(t_1)$ **akko** $i \in I \setminus \{k\}$ i $\operatorname{sgn}\big(p_i(t_1)\big) \cdot \operatorname{sgn}\big(p_{i+1}(t_1)\big) < 0$ (jer je $p_j(t_1) \neq 0$ za svako $j \in I$) **akko** $i \in I \setminus \{k\}$ i $\operatorname{sgn}\big(p_i(t_2)\big) \cdot \operatorname{sgn}\big(p_{i+1}(t_2)\big) < 0$ **akko** $i \in S(t_2)$ (jer je $p_j(t_2) \neq 0$ za svako $j \in I$). Dakle $S(t_1) = S(t_2)$, a otuda dobijamo i $W(t_1) = W(t_2)$. $\bullet$

Pomoćno tvrđenje 2. Neka su $u < y < \gamma < x < v$ tako da je $N \cap (u, \gamma) = \emptyset$ i $N \cap (\gamma, v) = \emptyset$. Tada važi:
- ako je $q(\gamma) \neq 0$ onda je $W(y) = W(\gamma) = W(x)$;
- ako je $q(\gamma) = 0$ onda je $W(y) = W(\gamma) + 1$ i $W(\gamma) = W(x)$.

Dokaz. Kako su polinomi neprekidne funkcije to za svako $i \in \{j \in I |\ p_j(\gamma) \neq 0\} =: R$ možemo izabrati po neko $\varepsilon_i > 0$ takvo da

$$\forall t \in (\gamma - \varepsilon_i, \gamma + \varepsilon_i)\ \big(p_i(t) > 0\big) \quad \text{ili} \quad \forall t \in (\gamma - \varepsilon_i, \gamma + \varepsilon_i)\ \big(p_i(t) > 0\big).$$

Neka su $y_0 \in (y,\gamma)$ i $x_0 \in (\gamma,x)$ takvi da je $|y_0-\gamma| < \min\limits_{i\in R}\varepsilon_i$ i $|x_0-\gamma| < \min\limits_{i\in R}\varepsilon_i$. Tada za svako $i \in R$ važi $\operatorname{sgn}\big(p_i(y_0)\big)= \operatorname{sgn}\big(p_i(\gamma)\big) = \operatorname{sgn}\big(p_i(x_0)\big) \neq 0$. Zato na osnovu Pomoćnog tvrđenja 1 mora biti:

$$\operatorname{sgn}\big(p_i(y)\big)= \operatorname{sgn}\big(p_i(\gamma)\big) = \operatorname{sgn}\big(p_i(x)\big) \neq 0,$$

$$\text{za svako } i \in I \text{ takvo da je } p_i(\gamma) \neq 0.$$

Označimo $I' := \{i \in I | 1 \leq i \leq k \ \wedge \ p_i(\gamma) = 0\}$ i, za $i \in I'$, $P_i := \{i-1, i\}$. Primetimo da $0 \notin I'$ čak iako možda važi $p_0(\gamma) = 0$.

Pokažimo najpre da je za $i, j \in I'$, $i \neq j \Rightarrow P_i \cap P_j = \emptyset$. Neka je, određenosti radi, $i < j$. Kad bi bilo $\{i-1, i\} \cap \{j-1, j\} \neq \emptyset$ onda bi imali $i = j-1$ ili $i = j$, pa kako je $i \neq j$ to je $i = j-1$, te je $p_{j-1}(\gamma) = p_i(\gamma) = 0$, jer $i \in I'$, što protivureči činjenici da $p_j(\gamma) = 0$ jer bi onda p_j i p_{j-1} imali zajednički koren γ.

Stavimo $P := \bigcup\limits_{i\in I'} P_i \supseteq I'$. [**Jedno jednostavno zapažanje:** Primetimo da je $0 \in P$ akko $p_1(\gamma) = 0$, u kom slučaju naravno mora biti $p_0(\gamma) \neq 0$].

Pokažimo:
• (1) Iz $i \in I \setminus P \ \wedge \ p_i(\gamma) \neq 0$ sledi

$$i \in S(y) \iff i \in S(\gamma) \quad \text{i} \quad i \in S(\gamma) \iff i \in S(x).$$

Zaista, kako je $p_i(\gamma) \neq 0$ to imamo

$$0 \neq \operatorname{sgn}\big(p_i(y)\big)= \operatorname{sgn}\big(p_i(\gamma)\big) = \operatorname{sgn}\big(p_i(x)\big).$$

Ako je $i = k$ onda $i \notin S(y)$, $i \notin S(\gamma)$ i $i \notin S(x)$, te gornje dve ekvivalencije važe. Neka je $i < k$. Tada $i+1 \in I$. Ako $p_{i+1}(\gamma) = 0$ onda $i+1 \in I'$ i $i \in P_{i+1} \subseteq P$, kontradikcija. Dakle mora biti $p_{i+1}(\gamma) \neq 0$. Zato je

$$0 \neq \operatorname{sgn}\big(p_{i+1}(y)\big)= \operatorname{sgn}\big(p_{i+1}(\gamma)\big) = \operatorname{sgn}\big(p_{i+1}(x)\big).$$

Odavde sada imamo: $p_i(y)\cdot p_{i+1}(y) < 0$ **akko** $p_i(\gamma)\cdot p_{i+1}(\gamma) < 0$ **akko** $p_i(x)\cdot p_{i+1}(x) < 0$. Drugim rečima $i \in S(y)$ **akko** $i \in S(\gamma)$ **akko** $i \in S(x)$. •

Pokažimo:
• (2) Iz $i \in I \setminus P \ \wedge \ 1 \leq i \leq k$ sledi

$$i \in S(y) \iff i \in S(\gamma) \quad \text{i} \quad i \in S(\gamma) \iff i \in S(x).$$

Ovo direktno proizilazi iz (1) jer za takvo i mora biti $p_i(\gamma) \neq 0$ obzirom da bi u suprotnom, zbog $1 \leq i \leq k$, imali $i \in I'$ te i $i \in P_i \subseteq P$. •

Pokažimo:
• (3) Ako $p_0(\gamma) \neq 0$ onda iz $i \in I \setminus P$ sledi

$$i \in S(y) \iff i \in S(\gamma) \quad \text{i} \quad i \in S(\gamma) \iff i \in S(x).$$

Neka je $i \in I \setminus P$. Ako $1 \leq i \leq k$ onda gornje dve ekvivalencije slede iz (2). Ako je $i = 0$ onda gornje dve ekvivalencije slede iz (1).•

Pokažimo:
• (4) Ako je $p_0(\gamma) = 0$ onda:
(a) $0 \notin P$;
(b) $0 \in S(y)$, $0 \notin S(\gamma)$ i $0 \notin S(x)$.

(a) je ustvari deo onog *Jednog jednostavnog zapažanja*: kad bi bilo $0 \in P$ onda bi iz $0 \in \{j-1, j\}$ i $j \in I'$ sledilo $j = 1 \in I'$ odakle je $p_1(\gamma) = 0$ pa bi p_0 i p_1 imali zajednički koren. Zato mora da važi (a).

Iz $p_0(\gamma) = 0$ direktno sledi $0 \notin S(\gamma)$. $p_0(\gamma) = 0$ takođe povlači prema uslovu (iv) iz definicije Šturmovog niza postoji $\epsilon > 0$ tako da $p_0(t)p_1(t) < 0$ za svako $t \in (\gamma - \epsilon, \gamma)$ i $p_0(t)p_1(t) > 0$ za svako $t \in (\gamma, \gamma + \epsilon)$. Neka su $y_1 \in (y, \gamma)$ i $x_1 \in (\gamma, x)$ takvi da je $|y_1 - \gamma| < \varepsilon$ kao i $|x_1 - \gamma| < \varepsilon$. Na osnovu Pomoćnog tvrđenja 1 imamo
- $0 \neq \operatorname{sgn}\big(p_0(y)\big) = \operatorname{sgn}\big(p_0(y_1)\big)$ i $0 \neq \operatorname{sgn}\big(p_1(y)\big) = \operatorname{sgn}\big(p_1(y_1)\big)$;
- $0 \neq \operatorname{sgn}\big(p_0(x)\big) = \operatorname{sgn}\big(p_0(x_1)\big)$ i $0 \neq \operatorname{sgn}\big(p_1(x)\big) = \operatorname{sgn}\big(p_1(x_1)\big)$.

Otuda je $0 \in S(y)$ **akko** $p_0(y) \cdot p_1(y) < 0$ **akko** $p_0(y_1) \cdot p_1(y_1) < 0$ **akko** $0 \in S(y_1)$. No $y_1 \in (\gamma - \varepsilon, \gamma)$ pa je $p_0(y_1) \cdot p_1(y_1) < 0$, tj. $0 \in S(y_1)$. Ovim smo pokazali $0 \in S(y)$.

Takođe je $0 \in S(x)$ **akko** $p_0(x) \cdot p_1(x) < 0$ **akko** $p_0(x_1) \cdot p_1(x_1) < 0$ **akko** $0 \in S(x_1)$. No $x_1 \in (\gamma, \gamma + \varepsilon)$ pa je $p_0(x_1) \cdot p_1(x_1) > 0$, tj. $0 \notin S(x_1)$. Ovim smo pokazali $0 \notin S(x)$. •

Pokažimo:
• (5) Ako je $i \in I'$ onda

$$\operatorname{card}\Big(S(y) \cap P_i\Big) = \operatorname{card}\Big(S(\gamma) \cap P_i\Big) = \operatorname{card}\Big(S(x) \cap P_i\Big) = 1.$$

Neka je $i \in I'$, drugim rečima $1 \leq i \leq k$ i $p_i(\gamma) = 0$. Jasno $i < k$, pa je $i + 1 \in I$. Takođe je $i - 1 \in I$. Zbog uslova (iii) iz definicije Šturmovog niza je $p_{i-1}(\gamma)p_{i+1}(\gamma) < 0$. Specijalno, zbog $p_i(\gamma) = 0$, imamo $i - 1 \in S(\gamma)$ i $i \notin S(\gamma)$ pa je $\operatorname{card}\Big(S(\gamma) \cap P_i\Big) = 1$. Kako je očigledno $p_{i-1}(\gamma) \neq 0$ i $p_{i+1}(\gamma) \neq 0$ to imamo da je

$$\operatorname{sgn}\big(p_{i-1}(y)\big) = \operatorname{sgn}\big(p_{i-1}(\gamma)\big) = \operatorname{sgn}\big(p_{i-1}(x)\big) =: s_0 \in \{-1, 1\}$$

i

$$\operatorname{sgn}\big(p_{i+1}(y)\big) = \operatorname{sgn}\big(p_{i+1}(\gamma)\big) = \operatorname{sgn}\big(p_{i+1}(x)\big) =: s_1 \in \{-1, 1\}.$$

Znamo da je $s_0 \cdot s_1 < 0$.

Stavimo $l := \operatorname{sgn}\big(p_i(y)\big)$ i $d := \operatorname{sgn}\big(p_i(x)\big)$. Jasno $\{l, d\} \subseteq \{-1, 1\}$.

Ako je $l \cdot s_0 > 0$ (odnosno $d \cdot s_0 > 0$) onda je $l \cdot s_1 < 0$ (odnosno $d \cdot s_1 < 0$) pa je $i - 1 \notin S(y)$ (odnosno $i - 1 \notin S(x)$) i $i \in S(y)$ (odnosno $i \in S(x)$). Ako je $l \cdot s_0 < 0$ (odnosno $d \cdot s_0 < 0$) onda je $l \cdot s_1 > 0$ (odnosno $d \cdot s_1 > 0$) pa je $i - 1 \in S(y)$ (odnosno $i - 1 \in S(x)$) i $i \notin S(y)$ (odnosno $i \notin S(x)$). U svakom slučaju je $\operatorname{card}\Big(S(y) \cap P_i\Big) = 1 = \operatorname{card}\Big(S(y) \cap P_i\Big)$. •

Konačno možemo pokazati i samo pomoćno tvrđenje 2.

- Neka je $q(\gamma) \neq 0$. Imamo

$$\operatorname{card}\big(S(y)\big) = \operatorname{card}\Big(S(y) \cap I\Big) = \operatorname{card}\Big(S(y) \cap [P \cup (I \setminus P)]\Big) =$$

$$\operatorname{card}\Big(S(y) \cap P\Big) + \operatorname{card}\Big(S(y) \cap (I \setminus P)\Big) =$$

$$\operatorname{card}\Big(S(y) \cap \bigcup_{i \in I'} P_i\Big) + \operatorname{card}\Big(S(y) \cap (I \setminus P)\Big) =$$

$$\operatorname{card}\Big(\bigcup_{i \in I'} (S(y) \cap P_i)\Big) + \operatorname{card}\Big(S(y) \cap (I \setminus P)\Big) =$$

$$\sum_{i \in I'} \operatorname{card}\Big(S(y) \cap P_i\Big) + \operatorname{card}\Big(S(y) \cap (I \setminus P)\Big) =$$

$$\operatorname{card}(I') + \operatorname{card}\Big(S(y) \cap (I \setminus P)\Big).$$

Na potpuno isti način pokazujemo da je

$$\operatorname{card}\big(S(\gamma)\big) = \operatorname{card}(I') + \operatorname{card}\Big(S(\gamma) \cap (I \setminus P)\Big)$$

i

$$\operatorname{card}\big(S(x)\big) = \operatorname{card}(I') + \operatorname{card}\Big(S(x) \cap (I \setminus P)\Big).$$

Ali iz (3) sledi da je u ovom slučaju $S(y) \cap (I \setminus P) = S(\gamma) \cap (I \setminus P) = S(x) \cap (I \setminus P)$. Otuda zaključujemo $\operatorname{card}\big(S(y)\big) = \operatorname{card}\big(S(\gamma)\big) = \operatorname{card}\big(S(x)\big)$, tj. $W(y) = W(\gamma) = W(x)$.

- Neka je sada $q(\gamma) = 0$. Označimo $J := I \setminus (P \cup \{0\})$. Znamo da je $0 \notin P$. Imamo

$$\operatorname{card}\big(S(y)\big) = \operatorname{card}\Big(S(y) \cap (\{0\} \cup P \cup J)\Big) =$$

$$\operatorname{card}\Big(S(y)\cap\{0\}\Big)+\sum_{i\in I'}\operatorname{card}\Big(S(y)\cap P_i\Big)+\operatorname{card}\Big(S(y)\cap J\Big)=$$

$$1+\operatorname{card}(I')+\operatorname{card}\Big(S(y)\cap J\Big).$$

Sa druge strane je

$$\operatorname{card}\big(S(\gamma)\big)=\operatorname{card}\Big(S(\gamma)\cap\{0\}\Big)+\sum_{i\in I'}\operatorname{card}\Big(S(\gamma)\cap P_i\Big)+\operatorname{card}\Big(S(\gamma)\cap J\Big)=$$

$$0+\operatorname{card}(I')+\operatorname{card}\Big(S(\gamma)\cap J\Big).$$

Na potpuno isti način pokazujemo da je

$$\operatorname{card}\big(S(x)\big)=0+\operatorname{card}(I')+\operatorname{card}\Big(S(x)\cap J\Big).$$

Zato, pošto je $S(y)\cap J=S(\gamma)\cap J=S(x)\cap J$ (na osnovu (2)), dobijamo da je $W(y)=W(\gamma)+1$ i $W(\gamma)=W(x)$. •

Prelazimo na dokaz same teoreme.

Slučaj 1: $(a,b)\cap N=\emptyset$. Neka je $r\in(a,b)$, proizvoljno.

Ako je $q(b)=0$ onda prema *Pomoćnom tvrđenju 2* mora biti

$$W(a)=W(r)\quad\text{ i }\quad W(r)=W(b)+1$$

pa je $W(a)-W(b)=1$, i pritom je $\{x\in(a,b]|\ q(x)=0\}=\{b\}$.

Ako je $q(b)\neq 0$ onda prema *Pomoćnom tvrđenju 2* mora biti

$$W(a)=W(r)=W(b)$$

pa je $W(a)-W(b)=0$, i pritom je $\{x\in(a,b]|\ q(x)=0\}=\emptyset$.

Slučaj 2: $(a,b)\cap N\neq\emptyset$. Tada postoje $m\in\mathbb{N}$ i $z_i\in\mathbb{R}$, $1\leq i\leq m$, tako da je $z_i<z_{i+1}$ za $1\leq i\leq m-1$, $a<z_1$, $z_m<b$ i $N\cap(a,b)=\{z_i|1\leq i\leq m\}$. Stavimo $z_0\overset{\text{df}}{:=}a$ i $z_{m+1}\overset{\text{df}}{:=}b$. Za svako $i=\overline{0,m}$ izaberimo po $r_i\in(z_i,z_{i+1})$ i neka su r_{m+1} i w realni brojevi takvi da je $b=z_{m+1}<r_{m+1}<w$ i tako da važi $N\cap(b,w)=\emptyset$. Imamo

$$W(a)-W(b)=W(z_0)-W(z_{m+1})=\sum_{i=0}^{m}\big(W(z_i)-W(z_{i+1})\big)=\sum_{i=0}^{m}\big(W(r_i)-W(r_{i+1})\big)$$

jer je $W(z_i)=W(r_i)$ za $i=\overline{0,m}$. Dalje kako je za $i=\overline{0,m}$

$$W(r_i)-W(r_{i+1})=\begin{cases}0, & \text{ako } q(z_{i+1})\neq 0,\\ 1, & \text{ako } q(z_{i+1})=0\end{cases}$$

to sada imamo

$$W(a) - W(b) = \operatorname{card}\Big(\big\{j \in \{1, \ldots, m+1\}|\ q(z_j) = 0\big\}\Big) =$$

$$= \operatorname{card}\Big(\{x \in (a, b]|\ q(x) = 0\}\Big),$$

obzirom da je $\{x \in (a, b)|\ q(x) = 0\} \subseteq N$. $\square$

Ukoliko polinom nema višestrukih korena onda ne samo da za njega postoji Šturmov niz već naredna teorema daje i efektivan postupak za njegovo nalaženje.

Teorema 7 Neka je q nekonstantan polinom sa realnim koeficijentima bez višestrukih korena. Niz polinoma $\langle p_i | 0 \leq i \leq k\rangle$ definisan tako da je:

$$p_0 = q,$$

$$p_1 = q',$$

$$p_{i+1} = -r_i, \text{ gde je } r_i \text{ ostatak pri deljenju polinoma } p_{i-1} \text{ polinomom } p_i,$$

$$p_k | p_{k-1}$$

je Šturmov niz za polinom q.

Dokaz. Najpre, na isti način kao kod Euklidovog algoritma za dva polinoma pokazuje se da se u ovako definisanom nizu dolazi do deljenja bez ostatka kao i da je $p_k = \lambda_0 \cdot \mathrm{NZD}(q, q') = \lambda_i \cdot \mathrm{NZD}(p_i, p_{i+1})$ za $1 \leq i < k$ i neke nenula realne brojeve λ_j, $0 \leq j < k$. Pokažimo da se zaista radi o Šturmovom nizu.
(i) Kad bi p_k imao neki realan koren onda bi, zbog $p_k = \lambda_0 \cdot \mathrm{NZD}(q, q')$, q imao višestruki koren, suprotno pretpostavci.
(ii) Ako bi, za neko $0 \leq i < k$, polinomi p_i i p_{i+1} imali zajednički koren α onda bi imali $(x - \alpha) | \lambda_i \cdot \mathrm{NZD}(p_i, p_{i+1}) = p_k$ pa bi p_k imao koren α, suprotno pokazanoj osobini (i).
(iii) Neka je, za neko $\alpha \in \mathbb{R}$ i neko $1 \leq i < k$, $p_i(\alpha) = 0$. Ako je m količnik pri deljenju p_{i-1} sa p_i, onda važi $p_{i-1} = m \cdot p_i - p_{i+1}$. Specijalno $p_{i-1}(\alpha) = -p_{i+1}(\alpha)$, pa, kako su ova dva broja različita od nule (na osnovu pokazane osobine (2)), imamo $p_{i-1}(\alpha) \cdot p_{i+1}(\alpha) < 0$.
(iv) Neka je $q(\alpha) = 0$. Kako je α jednostruki koren od q, a imajući u vidu da je (u skladu sa tim) $q'(\alpha) \neq 0$, postoji $\epsilon > 0$ i $s, l \in \{1, -1\}$ tako da je $\forall x \in (\alpha - \epsilon, \alpha)$ $(\mathrm{sgn}\big(q(x)\big) = s)$, $\forall x \in (\alpha, \alpha + \epsilon)$ $(\mathrm{sgn}\big(q(x)\big) = -s)$ i $\forall x \in (\alpha - \epsilon, \alpha + \epsilon)$ $(\mathrm{sgn}\big(q'(x)\big) = l)$. Imamo da je $\mathrm{sgn}\big(q(x)q'(x)\big) = s \cdot l$ za $x \in (\alpha - \epsilon, \alpha)$ i $\mathrm{sgn}\big(q(x)q'(x)\big) = -s \cdot l$ za $x \in (\alpha, \alpha + \epsilon)$.
Ako je $l = 1$ onda je q rastuća funkcija na $(\alpha - \epsilon, \alpha + \epsilon)$ pa mora biti $s = -1$. Zato je $s \cdot l = -1$ i $-s \cdot l = 1$.

Ako je $l = -1$ onda je q opadajuća funkcija na $(\alpha - \epsilon, \alpha + \epsilon)$ pa mora biti $s = 1$. Zato je ponovo $s \cdot l = -1$ i $-s \cdot l = 1$. $\square$

Ukoliko polinom q ima neki realan višestruki koren tada treba najpre izračunati najveći zajednički delilac polinoma q i q'. Ako je $l = \mathrm{NZD}(q, q')$, onda polinom $\frac{q}{l}$ nema višestruke korene dok su mu koreni isti kao i oni polinoma q. Zato primenjujući prethodno opisan algoritam na polinom $\frac{q}{l}$ možemo pronaći broj realnih korena polinoma q koje se nalaze u nekom datom s desna zatvorenom intervalu.

Primer. Neka je $q(x) = (x+1)x(x-1)(x-2)$. Primenjujući algoritam opisan u Teoremi 7 dobijamo:
$p_0(x) = x^4 - 2x^3 - x^2 + 2x$, $p_1(x) = 4x^3 - 6x^2 - 2x + 2$, $p_2(x) = x^2 - \frac{5}{4}x - \frac{1}{4}$, $p_3(x) = \frac{3}{2}x - \frac{7}{4}$ i $p_4(x) = \frac{25}{72}$. Ako za $x \in \mathbb{R}$ označimo

$$K(x) = \begin{bmatrix} \operatorname{sgn}\big(p_0(x)\big) \\ \operatorname{sgn}\big(p_1(x)\big) \\ \operatorname{sgn}\big(p_2(x)\big) \\ \operatorname{sgn}\big(p_3(x)\big) \\ \operatorname{sgn}\big(p_4(x)\big) \end{bmatrix}$$

onda imamo

$$K(-2) = \begin{bmatrix} +1 \\ -1 \\ +1 \\ -1 \\ +1 \end{bmatrix},\ K(-1) = \begin{bmatrix} 0 \\ -1 \\ +1 \\ -1 \\ +1 \end{bmatrix},\ K(0) = \begin{bmatrix} 0 \\ +1 \\ -1 \\ -1 \\ +1 \end{bmatrix},\ K\left(\frac{7}{6}\right) = \begin{bmatrix} +1 \\ -1 \\ -1 \\ 0 \\ +1 \end{bmatrix},$$

$$K(1) = \begin{bmatrix} 0 \\ -1 \\ -1 \\ -1 \\ +1 \end{bmatrix},\ K(2) = \begin{bmatrix} 0 \\ +1 \\ +1 \\ +1 \\ +1 \end{bmatrix} \quad \text{i} \quad K(4) = \begin{bmatrix} +1 \\ +1 \\ +1 \\ +1 \\ +1 \end{bmatrix}.$$

Odavde vidimo da je $S(-2) = \{0,1,2,3\}$, $S(-1) = \{1,2,3\}$, $S(0) = \{1,3\}$, $S\left(\frac{7}{6}\right) = \{0,2\}$, $S(1) = \{3\}$, $S(2) = \emptyset$ i $S(4) = \emptyset$, te i da je $W(-2) = 4$, $W(-1) = 3$, $W(0) = 2$, $W\left(\frac{7}{6}\right) = 2$, $W(1) = 1$, $W(2) = 0$ i $W(4) = 0$. Kako q nema višestrukih realnih korena to zaključak Teoreme 7 stoji. Možemo ga testirati na ovom konkretnom primeru. $\square$

V.2 Rezultanta dva polinoma

Rezultanta polinoma $p(x) = u \prod_{i=1}^{n}(x - \alpha_i)$ i $q(x) = v \prod_{i=1}^{m}(x - \beta_i)$, gde $u, v \in \mathbb{C} \setminus \{0\}$ i $\alpha_i, \beta_j \in \mathbb{C}$, jeste broj $Rez(p,q) := u^m v^n \prod \langle \alpha_i - \beta_j | i = \overline{1,n}, j = \overline{1,m} \rangle$.

Očigledno $Rez(p,q) = 0$ akko p i q imaju zajedničkih korena.

Neka je $p(x) = u \prod_{i=1}^{n}(x - \alpha_i) = a_n x^n + \cdots + a_1 x + a_0$ i
$q(x) = v \prod_{i=1}^{m}(x - \beta_i) = b_m x^m + \cdots + b_1 x + b_0$.
Označimo

$$A := \begin{bmatrix} \left.\begin{matrix} a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & a_3 & a_2 & a_1 & a_0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & a_n & \dots & a_4 & a_3 & a_2 & a_1 & a_0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & a_n & a_{n-1} & a_{n-2} & a_{n-3} & \dots\dots\dots & & & \dots & a_1 & a_0 \end{matrix}\right\} m \\ \\ \left.\begin{matrix} b_m & b_{m-1} & b_{m-2} & \dots & b_2 & b_1 & b_0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & b_m & b_{m-1} & \dots & b_3 & b_2 & b_1 & b_0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & b_m & \dots & b_4 & b_3 & b_2 & b_1 & b_0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & b_n & b_{n-1} & b_{n-2} & b_{n-3} & \dots\dots\dots & & & \dots & b_1 & b_0 \end{matrix}\right\} n \end{bmatrix}.$$

Rezultat kome je posvećen ovaj odeljak dat je, uz zadržavanje gornjih oznaka, narednom teoremom.

Teorema 8 $detA = Rez(p,q)$.

Dokaz. U dokazu ćemo koristiti dobro poznatu činjenicu da

$$V(x_1, \dots, x_k) := \begin{vmatrix} x_1^{k-1} & \dots & x_k^{k-1} \\ \vdots & \dots & \vdots \\ x_1^3 & \dots & x_k^3 \\ x_1^2 & \dots & x_k^2 \\ x_1 & \dots & x_k \\ 1 & \dots & 1 \end{vmatrix}$$

$$= \prod_{1\le i<j\le k}(x_i - x_j).$$

Uočimo matricu

$$M := \begin{bmatrix} \beta_1^{n+m-1} & \dots & \beta_m^{n+m-1} & \alpha_1^{n+m-1} & \dots & \alpha_n^{n+m-1} \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ \beta_1^3 & \dots & \beta_m^3 & \alpha_1^3 & \dots & \alpha_n^3 \\ \beta_1^2 & \dots & \beta_m^2 & \alpha_1^2 & \dots & \alpha_n^2 \\ \beta_1 & \dots & \beta_m & \alpha_1 & \dots & \alpha_n \\ 1 & \dots & 1 & 1 & \dots & 1 \end{bmatrix}.$$

Primetimo najpre da

$$[\ \underbrace{0\ 0\ \dots\ 0\ 0}_{m-k-1}\ a_n\ a_{n-1}\ \dots\ a_1\ a_0\ \ \underbrace{0\ 0\ \dots\ 0\ 0}_{k}\ ] \cdot \begin{bmatrix} \gamma^{n+m-1} \\ \vdots \\ \gamma^3 \\ \gamma^2 \\ \gamma \\ 1 \end{bmatrix} = [\gamma^k p(\gamma)]$$

kao i da

$$[\ \underbrace{0\ 0\ \dots\ 0\ 0}_{n-k-1}\ b_m\ b_{m-1}\ \dots\ b_1\ b_0\ \ \underbrace{0\ 0\ \dots\ 0\ 0}_{k}\ ] \cdot \begin{bmatrix} \gamma^{n+m-1} \\ \vdots \\ \gamma^3 \\ \gamma^2 \\ \gamma \\ 1 \end{bmatrix} = [\gamma^k q(\gamma)].$$

Koristeći ovu činjenicu imamo da je

$$A \cdot M = \begin{bmatrix} \beta_1^{m-1}p(\beta_1) & \dots & \beta_m^{m-1}p(\beta_m) & \alpha_1^{m-1}p(\alpha_1) & \dots & \alpha_n^{m-1}p(\alpha_n) \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ \beta_1^3 p(\beta_1) & \dots & \beta_m^3 p(\beta_m) & \alpha_1^3 p(\alpha_1) & \dots & \alpha_n^3 p(\alpha_n) \\ \beta_1^2 p(\beta_1) & \dots & \beta_m^2 p(\beta_m) & \alpha_1^2 p(\alpha_1) & \dots & \alpha_n^2 p(\alpha_n) \\ \beta_1 p(\beta_1) & \dots & \beta_m p(\beta_m) & \alpha_1 p(\alpha_1) & \dots & \alpha_n p(\alpha_n) \\ p(\beta_1) & \dots & p(\beta_m) & p(\alpha_1) & \dots & p(\alpha_n) \\ & & & & & \\ \beta_1^{n-1}q(\beta_1) & \dots & \beta_m^{n-1}q(\beta_m) & \alpha_1^{n-1}q(\alpha_1) & \dots & \alpha_n^{n-1}q(\alpha_n) \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ \beta_1^3 q(\beta_1) & \dots & \beta_m^3 q(\beta_m) & \alpha_1^3 q(\alpha_1) & \dots & \alpha_n^3 q(\alpha_n) \\ \beta_1^2 q(\beta_1) & \dots & \beta_m^2 q(\beta_m) & \alpha_1^2 q(\alpha_1) & \dots & \alpha_n^2 q(\alpha_n) \\ \beta_1 q(\beta_1) & \dots & \beta_m q(\beta_m) & \alpha_1 q(\alpha_1) & \dots & \alpha_n q(\alpha_n) \\ q(\beta_1) & \dots & q(\beta_m) & q(\alpha_1) & \dots & q(\alpha_n) \end{bmatrix}.$$

Kako su α_i nule polinoma p a β_j nule polinoma q to je zapravo

$$A \cdot M = \begin{bmatrix} \beta_1^{m-1}p(\beta_1) & \dots & \beta_m^{m-1}p(\beta_m) & & & \\ \vdots & \dots & \vdots & & & \\ \beta_1^3 p(\beta_1) & \dots & \beta_m^3 p(\beta_m) & & \mathbf{O}_{m\times n} & \\ \beta_1^2 p(\beta_1) & \dots & \beta_m^2 p(\beta_m) & & & \\ \beta_1 p(\beta_1) & \dots & \beta_m p(\beta_m) & & & \\ p(\beta_1) & \dots & p(\beta_m) & & & \\ & & & & & \\ & & & \alpha_1^{n-1}q(\alpha_1) & \dots & \alpha_n^{n-1}q(\alpha_n) \\ & & & \vdots & \dots & \vdots \\ & \mathbf{O}_{n\times m} & & \alpha_1^3 q(\alpha_1) & \dots & \alpha_n^3 q(\alpha_n) \\ & & & \alpha_1^2 q(\alpha_1) & \dots & \alpha_n^2 q(\alpha_n) \\ & & & \alpha_1 q(\alpha_1) & \dots & \alpha_n q(\alpha_n) \\ & & & q(\alpha_1) & \dots & q(\alpha_n) \end{bmatrix},$$

gde su sa $\mathbf{O}_{m\times n}$ i $\mathbf{O}_{n\times m}$ označene *nula* matrice formata, redom, $m \times n$ i $n \times m$. Otuda je

$$det(A\cdot M)=\prod_{j=1}^{m}p(\beta_j)\ \prod_{i=1}^{n}q(\alpha_i)\cdot\begin{vmatrix}\beta_1^{m-1} & \dots & \beta_m^{m-1} & & & \\ \vdots & \dots & \vdots & & & \\ \beta_1^3 & \dots & \beta_m^3 & & \mathbf{O}_{m\times n} & \\ \beta_1^2 & \dots & \beta_m^2 & & & \\ \beta_1 & \dots & \beta_m & & & \\ 1 & \dots & 1 & & & \\ & & & \alpha_1^{n-1} & \dots & \alpha_n^{n-1}\\ & & & \vdots & \dots & \vdots \\ & \mathbf{O}_{n\times m} & & \alpha_1^3 & \dots & \alpha_n^3\\ & & & \alpha_1^2 & \dots & \alpha_n^2\\ & & & \alpha_1 & \dots & \alpha_n\\ & & & 1 & \dots & 1\end{vmatrix}$$

$$=\prod_{j=1}^{m}p(\beta_j)\ \prod_{i=1}^{n}q(\alpha_i)\cdot V(\beta_1,\dots,\beta_m)\ V(\alpha_1,\dots,\alpha_n)=$$

$$\prod_{j=1}^{m}p(\beta_j)\ \prod_{i=1}^{n}q(\alpha_i)\ \prod_{1\le k<s\le m}(\beta_k-\beta_s)\ \prod_{1\le k<s\le n}(\alpha_k-\alpha_s)=$$

$$a_n^m\ b_m^n\ \prod_{i=\overline{1,n},j=\overline{1,m}}(\beta_j-\alpha_i)\ \prod_{i=\overline{1,n},j=\overline{1,m}}(\alpha_i-\beta_j)\ \prod_{1\le k<s\le m}(\beta_k-\beta_s)\ \prod_{1\le k<s\le n}(\alpha_k-\alpha_s),$$

jer je

$$\prod_{j=1}^{m}p(\beta_j)\ \prod_{i=1}^{n}q(\alpha_i)=\prod_{j=1}^{m}\left[a_n\ \prod_{i=1}^{n}(\beta_j-\alpha_i)\right]\ \prod_{i=1}^{n}\left[b_m\ \prod_{j=1}^{m}(\alpha_i-\beta_j)\right]=$$

$$a_n^m\ b_m^n\ \prod_{i=\overline{1,n},j=\overline{1,m}}(\beta_j-\alpha_i)\ \prod_{i=\overline{1,n},j=\overline{1,m}}(\alpha_i-\beta_j).$$

Sa druge strane je

$$det(A\cdot M)=detA\cdot detM=$$

$$detA\cdot V(\beta_1,\dots,\beta_m,\alpha_1\dots,\alpha_n)=$$

$$detA\cdot\ \prod_{1\le k<s\le m}(\beta_k-\beta_s)\ \prod_{1\le k<s\le n}(\alpha_k-\alpha_s)\ \prod_{i=\overline{1,n},j=\overline{1,m}}(\beta_j-\alpha_i).$$

Pretpostavimo najpre da je $\alpha_k \neq \alpha_s$, za $1 \leq k < s \leq n$, da je $\beta_k \neq \beta_s$, za $1 \leq k < s \leq m$, kao i da je $\alpha_i \neq \beta_j$ za $i = \overline{1,n},\ j = \overline{1,m}$. Izjednačavajući dva izraza za $det(A \cdot M)$ koja smo dobili i nakon skraćivanja odgovarajućih izraza (koji pod učinjenim pretpostavkama nisu jednaki nuli) dobijamo

$$detA = a_n^m\ b_m^n \prod_{i=\overline{1,n},j=\overline{1,m}} (\alpha_i - \beta_j),$$

tj. $detA = Rez(p,q)$. Pokažimo da dobijena jednakost važi i inače. Imajući u vidu Viete-ove veze, $detA$ zapravo predstavlja izraz $L(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ za odgovarajuću $L : \mathbb{C}^{n+m} \to \mathbb{C}$ neprekidnu funkciju. Izraz $Rez(p,q)$ takođe predstavlja broj $D(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ za odgovarajuću $D : \mathbb{C}^{n+m} \to \mathbb{C}$ neprekidnu funkciju. Ono što smo mi uspeli da pokažemo jeste da važi $L(z_1, \ldots, z_{n+m}) = D(z_1, \ldots, z_{n+m})$ za svako $(z_1, \ldots, z_{n+m}) \in \mathbb{C}^{n+m}$ za koje je $z_i \neq z_j$, $1 \leq i < j \leq n+m$. Dakle imamo da se ove dve funkcije poklapaju na skupu $S := \{(z_1, \ldots, z_{n+m}) \in \mathbb{C}^{n+m} |\ z_i \neq z_j,\ 1 \leq i < j \leq n+m\}$ koji je *gust* u $\mathbb{C}^{n+m}$, pa se, zbog svoje neprekidnosti, one poklapaju i na celom skupu $\mathbb{C}^{n+m}$, tj. $L = D$. Otuda imamo da $detA = Rez(p,q)$ važi za proizvoljna dva polinoma p i q. $\square$

V.3 O simetričnim polinomima više promenljivih

Neka je u ovom odeljku fiksiran $n \in \mathbb{N}$.

Označimo $\mathbf{S} := (\mathbb{N} \cup \{0\})^n$ i $\mathbf{S}' := \{s \in \mathbf{S} | s_i \geq s_{i+1},\ 1 \leq i < n\}$. Oznaku $\leq$ ćemo koristiti i za leksikografsko uređenje na skupu $\mathbf{S}$. $(\mathbf{S}, \leq)$ je dobro uređenje.

Za $s \in \mathbf{S}$ sa s_i, $i = \overline{1,n}$ cemo označavati i-tu komponentu od s, tj. $s = (s_1, \ldots, s_n)$. Element $l \in \mathbf{S}$ takav da je $l_i = 0$ za $1 \leq i \leq n$ označavaćemo sa $\overrightarrow{0}$.

Stav 45 Neka je $(A, \leq)$ dobro uređenje i $B \subseteq A$ neprazan skup takav da kad god za $x \in A$ važi $\{y \in A |\ y \neq x,\ y \leq x\} \subseteq B$ onda je i $x \in B$. Tada mora biti $B = A$.

Dokaz. Pretpostavimo da je $C := A \setminus B \neq \emptyset$. Tada postoji najmanji element skupa C, neka je to npr. x_0. Kad bi bilo $\{y \in A |\ y \neq x_0,\ y \leq x_0\} \subseteq B$ onda bi imali $x_0 \in B$ što je nemoguće. Zato postoji neko $y \in C$ tako da $y \neq x_0$ i $y \leq x_0$. Ali tada x_0 nije najmanji element skupa C, kontradikcija. Dakle mora biti $B = A$. □

Pod *polinomom od n promenljivih* $x_1, \ldots, x_n$ *nad poljem* $\mathbb{R}$ podrazumevamo (neformalno govoreći) izraz koji je suma konačno mnogo izraza oblika $r \cdot x_1^{s_1} \ldots x_n^{s_n}$ gde je $r \in \mathbb{R} \setminus \{0\}$ a s_i su nenegativni celi brojevi. Za $s = (s_1, \ldots, s_n) \in \mathbf{S}$ uvedimo oznaku $x^s := x_1^{s_1} \ldots x_n^{s_n}$. Tada je polinom p od promenljivih $x_1, \ldots, x_n$ zapravo izraz $\sum_{s \in A} a_s x^s$ za neki konačan neprazan $A \subseteq \mathbf{S}$, gde su $a_s \in \mathbb{R} \setminus \{0\}$. Izraz $0 \cdot x^{\overrightarrow{0}}$ ćemo nazivati *nula polinom* i označavati ga sa $\mathbf{0}$. U daljem tekstu reč *polinom* će označavati isključivo polinom od promenljivih $x_1, \ldots, x_n$.

Polinomi se sabiraju i množe na uobičajen (prirodan) način, pri čemu ovde nećemo formalno definisati te operacije, uzdajući se u zdravu intuiciju čitalaca.

Definišemo *stepen* nenula polinoma na sledeći način. Stepen nenula polinoma $p = \sum_{s \in A} a_s x^s$, gde je A neki konačan neprazan podskup od $\mathbf{S}$, definiše se kao najveći (u odnosu na leksikografsko uređenje $\leq$ na skupu $\mathbf{S}$) element skupa A. Stepen polinoma q označavamo sa $st(q)$. Za polinome $a_s x^s$, $s \in A$, kažemo da su *članovi* polinoma $p = \sum_{s \in A} a_s x^s$ a za njegov član $a_l x^l$, gde je $st(p) = l$, da je *najstariji*.

Neka su dati polinomi $q_1, \ldots, q_n$. Ako u polinomu $p = \sum_{s \in A} a_s x^s$ promenljivu x_i formalno zamenimo polinomom q_i, za $1 \leq i \leq n$, tako dobijeni izraz $\sum_{s \in A} a_s q_1^{s_1} \ldots q_n^{s_n}$ ili predstavlja $\mathbf{0}$ ili polinom $\sum_{s \in B} b_s x^s$ za neki konačan neprazan $B \subseteq \mathbf{S}$. Koji god da se od ta dva polinoma dobije, njega ćemo označavati sa $p(q_1, \ldots, q_n)$.

Primer. (1) Ako je $p = x_1^2 - x_2^2;\ q_1 = x_1 - x_2,\ q_2 = x_1 + x_2$ onda je $p(q_1, q_2) = -4x_1x_2$.
(2) Ako je $p = x_1 - x_2$ i $q_1 = q_2 = x_1$ onda je $p(q_1, q_2) = \mathbf{0}$. □

Polinom p je *simetričan* ako za svaku permutaciju τ skupa $\{1,\dots,n\}$ važi

$$p(x_{\tau(1)},\dots,x_{\tau(n)}) = p(x_1,\dots,x_n)\ (\equiv p)\,.$$

Primeri simetričnih polinoma su tzv. *elementarni simetrični polinomi* kojih ima n a koji se definišu na sledeći način:

$$\sigma_1 := \sum_{i=1}^{n} x_i$$

$$\sigma_k := \sum_{1\le j_1<\dots<j_{s-1}<j_s<\dots<j_k\le n} \left(\prod_{s=1}^{k} x_{j_s} \right)$$

$$\sigma_n := \prod_{i=1}^{n} x_i.$$

Stav 46 Ako su polinomi $p, q \neq \mathbf{0}$ onda je najstariji član polinoma pq proizvod najstarijih članova polinoma p i q; takođe je $st(pq) = st(p) + st(q)$ (ovo "$+$" se ovde odnosi na standardno pokoordinatno sabiranje n-torki realnih brojeva).

Dokaz. Neka je $st(p) =: l$, $st(q) =: t, p = \sum_{s\in A} a_s x^s$ i $q = \sum_{s\in B} b_s x^s$. Proizvod najstarijih članova polinoma p i q jeste polinom $a_l b_t \cdot x_1^{l_1+t_1} \dots x_n^{l_n+t_n}$ (gde je $a_l \neq 0 \neq b_t$). Neka je $u \in A$ i $v \in B$ tako da $(u,v) \neq (l,t)$. Znamo da je $u \le l$ i $v \le t$. Postoji $j \in \{1,\dots,n\}$ tako da važi $u_j \neq l_j \vee v_j \neq t_j$. Neka je i_0 najmanji takav broj. Kako je, za $1 \le j < i_0$, $u_j = l_j$ i $v_j = t_j$, i kako je $u \le l$ i $v \le t$, to mora biti $u_{i_0} \le l_{i_0}$ i $v_{i_0} \le t_{i_0}$, pa zbog $u_{i_0} \neq l_{i_0} \vee v_{i_0} \neq t_{i_0}$ zaključujemo da je $u_{i_0} + v_{i_0} < l_{i_0} + t_{i_0}$. Obzirom da je $u_j + v_j = l_j + t_j$ za $1 \le j < i_0$ konačno dobijamo da je $u + v < l + t$. Dakle proizvod najstarijih članova ima stepen $l + t = st(p) + st(q)$ koji je strogo veći od stepena proizvoda bilo kog drugog para članova. Sada direktno sledi tvrđenje stava. □

Stav 47 Ako je p proizvoljan a $q_1,\dots,q_n$ simetrični polinomi onda je polinom $p(q_1,\dots,q_n)$ simetričan.

Dokaz. Neka je $p(q_1,\dots,q_n) =: l$. Ako je τ bilo koja permutacija skupa $\{1,\dots,n\}$ onda je

$$l(x_{\tau(1)},\dots,x_{\tau(n)}) = p(q_1(x_{\tau(1)},\dots,x_{\tau(n)}),\dots,q_n(x_{\tau(1)},\dots,x_{\tau(n)})) =$$

$$p(q_1(x_1,\dots,x_n),\dots,q_n(x_1,\dots,x_n)) = l(x_1,\dots,x_n)$$

i stav je dokazan. □

Za polinom $p = \sum_{s\in A} a_s x^s$ kažemo da je *homogen* ako je $\sum_{i=1}^{n} u_i = \sum_{i=1}^{n} v_i$ za svako $u, v \in A$. Broj $\sum_{i=1}^{n} u_i$, koji ne zavisi od izbora $u \in A$, nazivamo *stepenom homogenosti* polinoma p.

Primetimo da ako su p i q homogeni polinomi istog stepena homogenosti $k \in \mathbb{N} \cup \{0\}$, i $M, N \in \mathbb{R}$, onda je polinom $Mp + Nq$ ili $\mathbf{0}$ ili homogen polinom stepena homogenosti k. Takođe, jasno je da je proizvod dva homogena polinoma i sam homogen.

Stav 48 Ako je p simetričan polinom i $st(p) = l$. Tada je $l_i \geq l_{i+1}$ za $1 \leq i < n$ (tj. $l \in \mathbf{S}'$).

Dokaz. Pretpostavimo suprotno, tj. da postoji $i_0 \in \{1, \ldots, n-1\}$ tako da je $l_{i_0} < l_{l_0+1}$. Posmatrajmo permutaciju τ skupa $\{1, \ldots, n\}$ definisanu sa: $\tau(i_0) = i_0 + 1$, $\tau(i_0 + 1) = i_0$ i $\tau(k) = k$ inače. Kako je $p(x_{\tau(1)}, \ldots, x_{\tau(n)}) = p(x_1, \ldots, x_n)$ to je izraz $a_l x^t$, za $t = (l_1, \ldots, l_{i_0-1}, l_{i_0+1}, l_{i_0}, l_{i_0+2}, \ldots, l_n)$, član polinoma p a sa druge strane je $t > l = st(p)$, protivurečnost. □

Definišimo funkciju $\Delta : \mathbf{S}' \to \mathbf{S}$ sa $\Delta((s_1, \ldots, s_n)) = (s_1 - s_2, s_2 - s_3, \ldots, s_i - s_{i+1}, \ldots, s_{n-1} - s_n, s_n)$.

Za polinome $q_1, \ldots, q_n$ i $t \in \mathbf{S}$ uvedimo oznaku: $\lfloor q_1, \ldots, q_n \rfloor^t = q_1^{t_1} \ldots q_n^{t_n}$.

Centralni rezultat ovog odeljka predstavljaju naredne dve teoreme.

Teorema 9 Ako je p simetričan homogen polinom stepena $l \in \mathbf{S}$ i stepena homogenosti $k_0 \in \mathbb{N} \cup \{0\}$, onda postoje $M_s \in \mathbb{R}$, za $s \in \mathbf{S}'$ takve da je $s \leq l$ i $\sum_{i=1}^{n} s_i = k_0$, tako da je

$$p = \sum \langle M_s \lfloor \sigma_1 \ldots \sigma_n \rfloor^{\Delta(s)} | s \in \mathbf{S}', s \leq l, \quad \sum_{i=1}^{n} s_i = k_0 \rangle.$$

Dokaz. Ako je $p = \mathbf{0}$ stvar je jasna.

Dokaz za $p \neq \mathbf{0}$ izvodimo indukcijom po stepenu polinoma p.

(Formalno govoreći, posmatramo skup $B \subseteq \mathbf{S}$ onih elemenata s uređenja $\mathbf{S}$ sa osobinom da kad god je simetričan homogen nenula polinom stepena $s \in \mathbf{S}$ on zadovoljava tvrđenje ove teoreme, a onda pokazujemo da skup B ispunjava uslove Stava 45.)

Ukoliko je $p \neq \mathbf{0}$ takav simetričan homogen da nema nenula simetričnih homogenih polinoma stepena manjeg od $st(p)$ onda mora biti da je $st(p) = \overrightarrow{0}$ a za ovakve polinome tvrđenje ove teoreme je tačno (traženo razlaganje je $p = Ax^{\overrightarrow{0}} = A \cdot \lfloor \sigma_1, \ldots, \sigma_n \rfloor^{\overrightarrow{0}}$).

Pretpostavimo da je tvrđenje teoreme tačno za sve nenula simetrične homogene polinome stepena manjeg od $l \in \mathbf{S}$.

Neka je Ax^l najstariji član simetričnog homogenog polinoma p stepena l. Najstariji član polinoma $\lfloor \sigma_1 \ldots \sigma_n \rfloor^{\Delta(l)}$ je proizvod sledećih polinoma:

$$
\begin{array}{ccccccccc}
x_1^{l_1-l_2}, & & & & & & & & \\
x_1^{l_2-l_3} & x_2^{l_2-l_3}, & & & & & & & \\
x_1^{l_3-l_4} & x_2^{l_3-l_4} & x_3^{l_3-l_4}, & & & & & & \\
\vdots & & & & & & & & \\
x_1^{l_i-l_{i+1}} & x_2^{l_i-l_{i+1}} & x_3^{l_i-l_{i+1}} & \ldots & x_i^{l_i-l_{i+1}}, & & & & \\
\vdots & & & & & & & & \\
x_1^{l_{n-1}-l_n} & x_2^{l_{n-1}-l_n} & x_3^{l_{n-1}-l_n} & \ldots & x_i^{l_{n-1}-l_n} & \ldots & x_{n-1}^{l_{n-1}-l_n}, & & \\
x_1^{l_n} & x_2^{l_n} & x_3^{l_n} & \ldots & x_i^{l_n} & \ldots & x_{n-1}^{l_n} & x_n^{l_n}
\end{array}
$$

tj. polinom x^l, pa su najstariji članovi polinoma p i $A \cdot \lfloor \sigma_1 \ldots \sigma_n \rfloor^{\Delta(l)}$ isti. Otuda je polinom $q := p - A \cdot \lfloor \sigma_1 \ldots \sigma_n \rfloor^{\Delta(l)}$ simetričan polinom koji, ako nije jednak $\mathbf{0}$, jeste stepena $t := st(q) < l$. Kako je $A \cdot \lfloor \sigma_1 \ldots \sigma_n \rfloor^{\Delta(l)}$ homogen polinom čiji je najstariji član Ax^l, to mu je stepen homogenosti upravo $\sum_{i=1}^{n} l_i = k_0$ – isti kao i za p. Zato je q ili $\mathbf{0}$ ili homogen polinom stepena homogenosti k_0. U prvom slučaju smo već dobili traženo razlaganje, a u drugom na polinom q primenjujemo indukcijsku hipotezu: postoje $N_s \in \mathbb{R}$, za $s \in \mathbf{S}'$ takve da je $s \leq t$ i $\sum_{i=1}^{n} s_i = k_0$, tako da je

$$q = \sum \langle N_s \lfloor \sigma_1 \ldots \sigma_n \rfloor^{\Delta(s)} | s \in \mathbf{S}', s \leq t, \quad \sum_{i=1}^{n} s_i = k_0 \rangle.$$

Tada je

$$p = A \cdot \lfloor \sigma_1 \ldots \sigma_n \rfloor^{\Delta(l)} +$$

$$\sum \langle N_s \lfloor \sigma_1 \ldots \sigma_n \rfloor^{\Delta(s)} | s \in \mathbf{S}', s \leq t, \quad \sum_{i=1}^{n} s_i = k_0 \rangle =$$

$$\sum \langle M_s \lfloor \sigma_1 \dots \sigma_n \rfloor^{\Delta(s)} | s \in \mathbf{S}', s \leq l, \quad \sum_{i=1}^{n} s_i = k_0 \rangle,$$

gde je za $s \in \mathbf{S}'$ takve da $s \leq l$ i $\sum_{i=1}^{n} s_i = k_0$ stavljeno: $M_s = A$ ako $s = l$; $M_s = N_s$ ako $s \leq t$; $M_s = 0$ inače.

Induktivnim rasuđivanjem zaključujemo da je tvrđenje teoreme tačno. □

Na gotovo identičan način se dokazuje i naredna teorema.

Teorema 10 Ako je p simetričan polinom stepena $l \in \mathbf{S}$, onda postoje $M_s \in \mathbb{R}$, za $s \in \mathbf{S}'$ takve da je $s \leq l$, tako da je

$$p = \sum \langle M_s \lfloor \sigma_1 \dots \sigma_n \rfloor^{\Delta(s)} | s \in \mathbf{S}', s \leq l \rangle. \quad \square$$