Polinomi u jednoj varijabli

Cvenić, Doris

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:120787

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski sveučilišni nastavnički studij matematike i informatike

Doris Cvenić

Polinomi u jednoj varijabli

Diplomski rad

Osijek, 2022.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski sveučilišni nastavnički studij matematike i informatike

Doris Cvenić

Polinomi u jednoj varijabli

Diplomski rad

Mentor: doc. dr. sc. Ljiljna Primorac Gajčić

Osijek, 2022.

Sadržaj

Uvod

Tema ovog rada su polinomi u jednoj varijabli. Polinomi su prve funkcije s kojima se učenici susreću tijekom svog obrazovanja i to u prvom razredu srednje škole učeći o linearnoj funkciji koja je polinom prvog stupnja. Kasnije se znanje o polinomima širi putem kvadratne funkcije koja je polinom drugog stupnja. Tek u četvrtom razredu srednje škole učenicima se definira pojam polinoma. To su funkcije koje imaju važnu ulogu u matematici, ali i u njenoj primjeni.

U prvom poglavlju definirat ćemo polinome n-tog stupnja, objasniti postupak zbrajanja i množenja polinoma te kako to utječe na stupanj polinoma. Nakon toga ćemo dokazati da je skup svih polinoma s tako definiranim operacijama prsten. Dokazat ćemo i teorem koji govori kada je neki polinom jednak nul-polinomu kako bi mogli dokazati teorem koji govori o tome kada su dva polinoma jednaka.

U sljedećem poglavlju definirat ćemo kada su polinomi djeljivi te iskazati i dokazati Teorem o dijeljenju s ostatkom. Na primjeru ćemo pokazati postupak dijeljenja polinoma. Kako bi jednostavnije podijelili polinom linearnim polinomom $(x - \alpha)$, objasnit ćemo taj postupak koristeći Hornerov algoritam i pokazati ga na primjeru. Nakon toga, definirat ćemo najveću zajedničku mjeru dvaju polinoma te dokazati da ona postoji i da je jedinstvena. Postupak traženja najveće zajedničke mjere opisat ćemo Euklidovim algoritmom te također pokazati na primjeru.

Još jedan bitan pojam su nultočke polinoma pa ćemo ih u trećem poglavlju definirati i dokazati teoreme vezane uz njih i faktorizaciju polinoma. Potom ćemo dokazati Viètеov teorem koji nam je koristan kako u nekim slučajevima ne bi morali određivati nultočke polinoma. Korištenje Viètеovih formula pokazat ćemo na primjeru.

U četvrtom poglavlju definirat ćemo algebarske jednadžbe jer svakoj od njih možemo pridružiti polinom, pa je njeno rješenje nultočka pripadnog polinoma. Zatim ćemo dati kratki povijesni pregled proučavanja algebarskih jednadžbi. Za lakše traženje rješenja algebarskih jednadžbi opisat ćemo i prikazati postupke traženja cjelobrojnih, racionalnih i kompleksnih rješenja.

Sljedeće svojstvo polinoma, koje ćemo objasniti u petom poglavlju, je reducibilnost i ireducibilnost polinoma. Iskazat ćemo i dokazati teoreme o ireducibilnosti nad $\mathbb{R}$ i $\mathbb{C}$ te reducibilnosti nad $\mathbb{Q}$.

U posljednjem, šestom poglavlju, definirat ćemo derivaciju polinoma i dokazati njena svojstva. Na primjerima ćemo pokazati traženje derivacije polinoma i korištenje njenih svojstava.

1 Pojam polinoma

U ovom poglavlju definirat ćemo polinome i iskazati i dokazati osnovna svojstva vezana uz njih koja će biti prikazana na primjerima. Definicije i tvrdnje iz ovog poglavlja mogu se pronaći u [1] i [6].

Definicija 1.1. *Funkciju* $p : \mathbb{R} \to \mathbb{R}$ *danu s*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \tag{1.1}$$

gdje su $a_0, a_1, \ldots, a_n \in \mathbb{R}$ *pri čemu je* $a_n \neq 0$ *i* $n \in \mathbb{N}$ *zovemo* ***polinom*** n***-tog stupnja*** *(nad* $\mathbb{R}$*).*

Zapis (1.1) *zovemo* ***kanonski zapis*** *polinoma* p*, a polinom* n*-tog supnja možemo još zapisati kao*

$$\sum_{i=0}^{n} a_i x^i. \tag{1.2}$$

Brojeve $a_i, i = 0, 1, \ldots, n$ *zovemo* ***koeficijenti polinoma****.*

Koeficijent a_0 *zovemo* ***slobodni član*** *polinoma* p*, a koeficijent* a_n ***vodeći koeficijent*** *polinoma* p*.*

Ako je $p \neq 0$ *onda broj* n *zovemo* ***stupanj polinoma*** *i to zapisujemo kao* $\operatorname{st} p = n$*.*

Ako je $a_n = 1$ *onda polinom* p *zovemo* ***normiran polinom****.*

Ako je $p(x) = 0$ *za sve* $x \in \mathbb{R}$ *onda polinom* p *zovemo* ***nul-polinom*** *i zapisujemo* $p = 0$*. Stupanj nul-polinoma se ne definira.*

Polinom oblika $p(x) = a$*, gdje je* $a \in \mathbb{R} \setminus \{0\}$*, zovemo* ***konstantni polinom*** *ili* ***konstanta*** *i zapisujemo* $p = a$*. Stupanj konstantnog polinoma je 0. Skup svih polinoma* $p : \mathbb{R} \to \mathbb{R}$ *označavamo sa* $\mathbb{R}[x]$*.*

Ako imamo dva polinoma p i q onda su oni funkcije definirane na istom skupu brojeva, što znači da operacije zbrajanja i množenja definiramo kao pripadne operacije na funkcijama na sljedeći način:

$$(p + q)(x) := p(x) + q(x)$$
$$(pq)(x) := p(x)q(x).$$

Zapišemo li polinome p i q kao

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i,$$

$$q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 = \sum_{i=0}^{m} b_i x^i,$$

možemo pokazati da su $p+q$ i pq također polinomi. Uzmimo da je na primjer $n \geq m$. Tada vrijedi:

$$\begin{aligned}(p+q)(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_{m+1}x^{m+1} + (a_m + b_m)x^m + \\ &\quad + \cdots + (a_1 + b_1)x + a_0 + b_0 \\ &= \sum_{i=m+1}^{n} a_i x^i + \sum_{i=0}^{m}(a_i + b_i)x^i.\end{aligned}$$

$$\begin{aligned}(pq)(x) &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0)\\ &= a_n b_m x^n x^m + (a_n b_{m-1} + a_{n-1}b_m)x^n x^{m-1} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0\\ &= a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1}b_m)x^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0\\ &= \sum_{i=0}^{n+m}\Big(\sum_{k+j=i} a_k b_j\Big)x^i.\end{aligned}$$

Dakle, dva polinoma se zbrajaju tako da se zbroje članovi istog stupnja, a množe tako da se svaki član jednog polinoma pomnoži sa svakim članom drugog polinoma i dobiveni umnošci zbroje. Uočavamo da su zbroj i umnožak polinoma također polinomi.

Nadalje, uz pomoć osnovnih svojstava operacija zbrajanja i množenja polinoma dokazat ćemo tvrdnje u nastavku.

Propozicija 1.1. *(Vidjeti [1, Propozicija 7.3]) Funkcija* $\mathrm{st} : \mathbb{R}[x] \setminus \{0\} \to \mathbb{N}_0$ *zadovoljava sljedeća svojstva:*

1. $\mathrm{st}(pq) = \mathrm{st}p + \mathrm{st}q$
2. $\mathrm{st}(p+q) \leq \max\{\mathrm{st}p, \mathrm{st}q\}$
3. $\mathrm{st}(p \circ q) = \mathrm{st}p \cdot \mathrm{st}q$.

Dokaz. Prva jednakost je posljedica izraza za pq. Pretpostavimo da su a_n i b_m vodeći koeficijenti polinoma p i q. Tada je vodeći član od pq jednak $a_n b_m x^{n+m}$, pa je potencija tog polinoma jednaka zbroju stupnja polinoma p i polinoma q.
Druga nejednakost je posljedica izraza za $p+q$. Neka je stupanj polinoma p jednak n, a stupanj polinoma q jednak m. Ovdje razlikujemo tri slučaja:
1. slučaj: $n > m$
Zbrajanjem polinoma dobijemo da je vodeći član zbroja $p+q$ jednak $a_n x^n$ pa je stupanj zbroja jednak n.
2. slučaj: $n < m$
Zbrajanjem polinoma dobijemo da je vodeći član zbroja $p+q$ jednak $b_m x^m$ pa je stupanj polinoma jednak m.
3. slučaj: $n = m$
Zbrajanjem polinoma dobijemo da je vodeći član zbroja $p+q$ jednak $(a_n + b_n)x^n$. Vidimo da je stupanj zbroja jednak n ukoliko koeficijenti a_n i b_n nisu suprotni brojevi. Ako su koeficijenti a_n i b_n suprotni brojevi onda je stupanj zbroja manji od n.
Da bi dokazali treću jednakost pogledajmo izraz za $p \circ q$:

$$\begin{aligned}(p \circ q)(x) &= \sum_{i=0}^{n}\left(a_i(\sum_{j=0}^{m} b_j x^j)^i\right)\\ &= a_n(b_m x^m + \cdots + b_0)^n + a_{n-1}(b_m x^m + \cdots + b_0)^{n-1} +\\ &\quad + \cdots + a_1(b_m x^m + \cdots + b_0) + a_0\end{aligned}$$

Vidimo da je vodeći član od $p \circ q$ jednak $a_n (b_m)^n x^{nm}$ pa iz toga slijedi tvrdnja. □

Na sljedećim primjerima pokazat ćemo zbrajanje, množenje i određivanje kompozicije polinoma.

Primjer 1.1. *Odredite zbroj polinoma* $p(x) = 4x^2 + 5x - 3$ *i* $q(x) = x^4 + 2x^2 + 6$.

$$\begin{aligned}(p+q)(x) &= p(x) + q(x) \\ &= 4x^2 + 5x - 3 + x^4 + 2x^2 + 6 \\ &= x^4 + 6x^2 + 5x + 3\end{aligned}$$

Vidimo da je st $p = 2$ i st $q = 4$, a st $(p + q) = 4$. Dakle, zbrajanjem polinoma dobili smo polinom čiji je stupanj jednak stupnju polinoma q koji je većeg stupnja.

Primjer 1.2. *Odredite umnožak polinoma* $p(x) = 2x^2 + 3x - 2$ *i* $q(x) = x^3 + 3x^2 + 5$.

$$\begin{aligned}(pq)(x) &= p(x)q(x) \\ &= (2x^2 + 3x - 2)(x^3 + 3x^2 + 5) \\ &= 2x^2(x^3 + 3x^2 + 5) + 3x(x^3 + 3x^2 + 5) - 2(x^3 + 3x^2 + 5) \\ &= 2x^5 + 6x^4 + 10x^2 + 3x^4 + 9x^3 + 115x - 2x^3 - 6x^2 - 10 \\ &= 2x^5 + 9x^4 + 7x^3 + 4x^2 + 15x - 10\end{aligned}$$

Ovdje vidimo da je st $p = 2$ i st $q = 3$ te da smo množenjem polinoma p i q dobili polinom čiji je stupanj jednak zbroju stupnjeva polinoma koje množimo.

Primjer 1.3. *Odredite kompoziciju polinoma* $p(x) = 5x^2 + x + 4$ *i* $q(x) = x + 1$.

$$\begin{aligned}(p \circ q)(x) &= p(q(x)) \\ &= 5(x+1)^2 + (x+1) + 4 \\ &= 5(x^2 + 2x + 1) + x + 1 + 4 \\ &= 5x^2 + 10x + 5 + x + 5 \\ &= 5x^2 + 11x + 10\end{aligned}$$

Kompozicijom danih polinoma dobili smo polinom čiji je stupanj jednak umnošku stupnjeva polinoma p i q.

1.1 Prsten polinoma

Nakon što smo definirali zbrajanje i množenje polinoma, iskazat ćemo i dokazati propoziciju koja govori da je skup polinoma s tako definiranim zbrajanjem i množenjem prsten.

Propozicija 1.2. *(Vidjeti [5, Teorem 2.1.2])* $(\mathbb{R}[x], +, \cdot)$ *je komutativni prsten s jedinicom* $e(x) = 1$.

Dokaz. Prvo ćemo pokazati da je skup svih polinoma $p : \mathbb{R} \to \mathbb{R}$ prsten polinoma u jednoj varijabli x nad $\mathbb{R}$.
Elemente skupa p zapisat ćemo pomoću nizova koeficijenata polinoma $(a_0, a_1, a_2, \dots)$ takvih da je $a_i = 0$ za sve osim za konačno mnogo članova niza.

1. Asocijativnost zbrajanja
   Neka su $p, q, r \in \mathbb{R}[x]$ takvi da je $p = (a_0, a_1, a_2, \dots), q = (b_0, b_1, b_2, \dots)$ i $r = (c_0, c_1, c_2, \dots)$.

$$\begin{aligned} p + (q + r) &= (a_0, a_1, a_2, \dots) + ((b_0, b_1, b_2, \dots) + (c_0, c_1, c_2, \dots)) \\ &= (a_0, a_1, a_2, \dots) + (b_0 + c_0, b_1 + c_1, b_2 + c_2, \dots) \\ &= (a_0 + (b_0 + c_0), a_1 + (b_1 + c_1), a_2 + (b_2 + c_2), \dots) \\ (p + q) + r &= ((a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots)) + (c_0, c_1, c_2, \dots) \\ &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) + (c_0, c_1, c_2, \dots) \\ &= ((a_0 + b_0) + c_0, (a_1 + b_1) + c_1, (a_2 + b_2) + c_2, \dots) \end{aligned}$$

   Kako vrijedi asocijativnost elemenata iz prstena $\mathbb{R}$, dobiveni izrazi su jednaki.

2. Neutralni element
   $\exists 0 \in \mathbb{R}[x]$ tako da je $0 + p = p + 0 = p$.

$$\begin{aligned} (0, 0, 0, \dots) + (a_0, a_1, a_2, \dots) &= (0 + a_0, 0 + a_1, 0 + a_2, \dots) \\ &= (a_0, a_1, a_2, \dots) \\ (a_0, a_1, a_2, \dots) + (0, 0, 0, \dots) &= (a_0 + 0, a_1 + 0, a_2 + 0, \cdots) \\ &= (a_0, a_1, a_2, \dots) \end{aligned}$$

   Dakle, postoji neutralni element za zbrajanje.

3. Suprotni element
   $\forall p \in \mathbb{R}[x]$, $\exists -p \in \mathbb{R}[x]$ tako da je $p + (-p) = (-p) + p = 0$

$$\begin{aligned} p + (-p) &= (a_0, a_1, a_2, \dots) + (-a_0, -a_1, -a_2, \dots) \\ &= (a_0 + (-a_0), a_1 + (-a_1), a_2 + (-a_2), \dots) \\ &= (0, 0, 0, \dots) \end{aligned}$$

4. Komutativnost zbrajanja
   $p + q = q + p, \quad \forall p, q \in \mathbb{R}[x]$

$$\begin{aligned} p + q &= (a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) \\ &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) \\ q + p &= (b_0, b_1, b_2, \dots) + (a_0, a_1, a_2, \dots) \\ &= (b_0 + a_0, b_1 + a_1, b_2 + a_2, \dots) \end{aligned}$$

   Kako vrijedi komutativnost elemenata iz prstena $\mathbb{R}$, dobiveni izrazi su jednaki.

5. Asocijativnost množenja
   $p \cdot (q \cdot r) = (p \cdot q) \cdot r, \quad \forall p, q, r \in \mathbb{R}[x]$
   Neka je $(p \cdot q) \cdot r = e \cdot r = f$. Tada imamo:

$$\begin{aligned} e_n &= \sum_{k=0}^{n} a_k b_{n-k} \\ f_n &= \sum_{i=0}^{n} e_i c_{n-i} \\ &= \sum_{i=0}^{n} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) c_{n-i} \\ &= \sum_{i=0}^{n} \sum_{k=0}^{i} a_k b_{i-k} c_{n-i} \end{aligned}$$

   Neka je $p \cdot (q \cdot r) = p \cdot g = h$. Tada imamo:

$$\begin{aligned} g_n &= \sum_{k=0}^{n} b_k c_{n-k} \\ h_n &= \sum_{i=0}^{n} a_i g_{n-i} \\ &= \sum_{i=0}^{n} a_i \left(\sum_{k=0}^{n-i} c_{n-i-k} \right) \\ &= \sum_{i=0}^{n} \sum_{k=0}^{n-i} a_i b_k c_{n-i-k} \end{aligned}$$

   Pogledajmo je li $f_n = h_n$.

$$\begin{aligned} f_n &= \sum_{i=0}^{n} \sum_{k=0}^{i} a_k b_{i-k} c_{n-i} \\ &= \sum_{k=0}^{n} \sum_{i=k}^{n} a_k b_{i-k} c_{n-i} \\ &= \sum_{k=0}^{n} \sum_{i=0}^{n-k} a_k b_i c_{n-(k+i)} \end{aligned}$$

   Dakle, za $k = i$ vrijedi da je $f_n = h_n$.

6. Distributivnost slijeva i zdesna
   $p \cdot (q + r) = p \cdot q + p \cdot r$, $(p + q) \cdot r = p \cdot r + q \cdot r$, $\forall p, q, r \in \mathbb{R}[x]$

$$\begin{aligned}
p \cdot (q + r) &= (a_0, a_1, a_2, \dots) \cdot ((b_0, b_1, b_2, \dots) + (c_0, c_1, c_2, \dots)) \\
&= (a_0, a_1, a_2, \dots) \cdot (b_0 + c_0, b_1 + c_1, b_2 + c_2, \dots) \\
&= (a_0 \cdot (b_0 + c_0), a_1 \cdot (b_0 + c_0) + a_0 \cdot (b_1 + c_1), \dots) \\
&= (a_0 \cdot b_0 + a_0 \cdot c_0, a_1 \cdot b_0 + a_1 \cdot c_0 + a_0 \cdot b_1 + a_0 \cdot c_1, \dots) \\
p \cdot q + p \cdot r &= (a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) + (a_0, a_1, a_2, \dots) \cdot (c_0, c_1, c_2, \dots) \\
&= (a_0 \cdot b_0, a_1 \cdot b_0 + a_0 \cdot b_1, \dots) + (a_0 \cdot c_0, a_1 \cdot c_0 + a_0 \cdot c_1, \dots) \\
&= (a_0 \cdot b_0 + a_0 \cdot c_0, a_1 \cdot b_0 + a_0 \cdot b_1 + a_1 \cdot c_0 + a_0 \cdot c_1, \dots)
\end{aligned}$$

   Kako za elemente iz prstena $\mathbb{R}$ vrijedi komutativnost obzirom na operaciju $+$, dobiveni izrazi su jednaki, odnosno vrijedi distributivnost slijeva.

$$\begin{aligned}
(p + q) \cdot r &= ((a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots)) \cdot (c_0, c_1, c_2, \dots) \\
&= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots) \cdot (c_0, c_1, c_2, \dots) \\
&= ((a_0 + b_0) \cdot c_0, (a_1 + b_1) \cdot c_0 + (a_0 + b_0) \cdot c_1, \dots) \\
&= (a_0 \cdot c_0 + b_0 \cdot c_0, a_1 \cdot c_0 + b_1 \cdot c_0 + a_0 \cdot c_1 + b_0 \cdot c_1, \dots) \\
p \cdot r + q \cdot r &= (a_0, a_1, a_2, \dots) \cdot (c_0, c_1, c_2, \dots) + (b_0, b_1, b_2, \dots) \cdot (c_0, c_1, c_2, \dots) \\
&= (a_0 \cdot c_0, a_1 \cdot c_0 + a_0 \cdot c_1, \dots) + (b_0 \cdot c_0, b_1 \cdot c_0 + b_0 \cdot c_1, \dots) \\
&= (a_0 \cdot c_0 + b_0 \cdot c_0, a_1 \cdot c_0 + a_0 \cdot c_1 + b_1 \cdot c_0 + b_0 \cdot c_1, \dots)
\end{aligned}$$

   Ovdje također vrijedi da su dobiveni izrazi jednaki zbog komutativnosti elemenata iz prstena $\mathbb{R}$ obzirom na operaciju $+$.

Nadalje, da bi $\mathbb{R}[x]$ bio komutativan prsten, za $p, q \in \mathbb{R}[x]$ treba vrijediti $p \cdot q = q \cdot p$.

$$\begin{aligned}
p \cdot q &= (a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) \\
&= (a_0 \cdot b_0, a_1 \cdot b_0 + a_0 \cdot b_1, \dots) \\
q \cdot p &= (b_0, b_1, b_2, \dots) \cdot (a_0, a_1, a_2, \dots) \\
&= (b_0 \cdot a_0, b_1 \cdot a_0 + b_0 \cdot a_1, \dots)
\end{aligned}$$

Kako su elementi iz $\mathbb{R}$ komutativni obzirom na operacije $+$ i $\cdot$, dobiveni izrazi su jednaki pa je $\mathbb{R}[x]$ komutativan prsten.

Da bi $\mathbb{R}[x]$ bio prsten s jedinicom mora postojati jedinstveni element $e \in \mathbb{R}[x]$ takav da vrijedi $e \cdot a = a \cdot e = a$.

$$\begin{aligned}
a \cdot e = a &\Leftrightarrow (a_0, a_1, a_2, \dots) \cdot (e_0, e_1, e_2, \dots) = (a_0, a_1, a_2, \dots) \\
&\Leftrightarrow (a_0 \cdot e_0, a_1 \cdot e_0 + a_0 \cdot e_1, a_2 \cdot e_0 + a_1 \cdot e_1 + a_0 \cdot e_2, \dots) = (a_0, a_1, a_2, \dots) \\
&\Leftrightarrow a_0 \cdot e_0 = a_0 \quad \wedge \quad a_1 \cdot e_0 + a_0 \cdot e_1 = a_1 \quad \wedge \quad a_2 \cdot e_0 + a_1 \cdot e_1 + a_0 \cdot e_2 = a_2 \quad \wedge \quad \dots \\
&\Leftrightarrow e_0 = 1 \quad \wedge \quad e_1 = 0 \quad \wedge \quad e_2 = 0 \quad \wedge \quad \dots \\
&\Leftrightarrow e = (1, 0, 0, \dots) \\
e \cdot a = a &\Leftrightarrow (e_0, e_1, e_2, \dots) \cdot (a_0, a_1, a_2, \dots) = (a_0, a_1, a_2, \dots) \\
&\Leftrightarrow (e_0 \cdot a_0, e_1 \cdot a_0 + e_0 \cdot a_1, e_2 \cdot a_0 + e_1 \cdot a_1 + e_0 \cdot a_2, \dots) = (a_0, a_1, a_2, \dots) \\
&\Leftrightarrow e_0 \cdot a_0 = a_0 \quad \wedge \quad e_1 \cdot a_0 + e_0 \cdot a_1 = a_1 \quad \wedge \quad e_2 \cdot a_0 + e_1 \cdot a_1 + e_0 \cdot a_2 = a_2 \quad \wedge \quad \dots \\
&\Leftrightarrow e_0 = 1 \quad \wedge \quad e_1 = 0 \quad \wedge \quad e_2 = 0 \quad \wedge \quad \dots \\
&\Leftrightarrow e = (1, 0, 0, \dots)
\end{aligned}$$

Dakle, $e = (1, 0, 0, \dots)$ je neutralni element u $\mathbb{R}[x]$.
Time smo pokazali da je $(\mathbb{R}[x], +, \cdot)$ komutativni prsten s jedinicom $e(x) = 1$. □

Napomena 1.1. *Može se uočiti da prethodne definicije i tvrdnje imaju smisla i ako* $\mathbb{R}$ *zamijenimo općenitim komutativnim prstenom s jedinicom* $\mathbb{P}$. *Specijalno, imamo prsten polinoma* $\mathbb{Z}[x]$ *nad cijelim brojevima* $\mathbb{Z}$, *prsten polinoma* $\mathbb{Q}[x]$ *nad poljem racionalnih brojeva* $\mathbb{Q}$ *i prsten polinoma* $\mathbb{C}[x]$ *nad poljem kompleksnih brojeva* $\mathbb{C}$.

1.2 Jednakost polinoma

U ovom potpoglavlju definirat ćemo kada su polinomi jednaki te iskazati i dokazati Teorem o nul-polinomu kako bi mogli dokazati Teorem o jednakosti. Definicija i tvrdnje u nastavku mogu se pronaći u [1] i [6].

Definicija 1.2. *Polinomi* $p, q \in \mathbb{R}[x]$ *su* ***jednaki*** *ako su jednaki kao funkcije, odnosno ako vrijedi* $p(x) = q(x), \forall x \in \mathbb{R}$.

Teorem 1.1. (O nul-polinomu) *(Vidjeti [1, Teorem 7.6]) Polinom* $p(x) = \sum_{i=0}^{n} a_i x^i$, *gdje su* $a_0, a_1, \dots, a_n \in \mathbb{R}$ *jednak je nul-polinomu ako i samo ako su* $a_i = 0$, $i = 0, 1, \dots, n$.

Dokaz.

$\Leftarrow$ Ako su svi $a_i = 0$ onda je očito da je $p(x) = 0, \forall x \in \mathbb{R}$.

$\Rightarrow$ Pokažimo sada obrat tako što ćemo dokaz svesti na kontradikciju. Pretpostavimo da je $p(x) = 0$, $x \in \mathbb{R}$ i da nisu svi koeficijenti jednaki nula te da je a_m najmanji takav koji je različit od nule. Tada vrijedi $a_0 = a_1 = a_2 = \cdots = a_{m-1} = 0$ i $a_m \neq 0$. Uzmimo da je $p = n - m$ i $b_0 = a_m, b_1 = a_{m+1}, \dots, b_p = a_{m+p} = a_n$. Sada polinom p možemo zapisati na sljedeći način:

$$p(x) = b_0 x^m + b_1 x^{m+1} + \cdots + b_p x^n = 0, \quad x \in \mathbb{R}. \tag{1.3}$$

Kada (1.3) podijelimo sa x^m $(x \neq 0)$ dobivamo:

$$b_0 + b_1 x + \cdots + b_p x^p = 0. \tag{1.4}$$

Sada ćemo ocijeniti koeficijent $|b_0|$ i pokazati da je b_0 manji od proizvoljnog pozitivnog realnog broja. Definirajmo

$$M := \max\{|b_0|, |b_1|, \dots, |b_p|\} > 0.$$

Uzmimo za vrijednosti $x \in \langle 0, \frac{1}{2}\rangle$. Tada vrijedi:

$$\begin{aligned}
|b_0| &= |-b_1x - \cdots - b_px^p| \\
&= |b_1xb \cdots + b_px^p| \\
&\leq |b_1|x + |b_2|x^2 + \cdots + |b_p|x^p \\
&\leq Mx(1 + x + \cdots + x^{p-1}) \\
&< Mx\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{p-1}}\right) \\
&= Mx\frac{1 - \frac{1}{2^p}}{1 - \frac{1}{2}} \\
&= 2Mx\left(1 - \frac{1}{2^p}\right) \\
&< 2Mx
\end{aligned}$$

Dakle, zaključujemo da za svaki $x \in \langle 0, \frac{1}{2}\rangle$ vrijedi $|b_0| < 2Mx$. Odnosno $\frac{|b_0|}{2M} < x$. Kako je $|b_0| \leq M$ imamo $\frac{|b_0|}{4M} \leq \frac{1}{4} < \frac{1}{2}$. Slijedi da gornja nejednakost vrijedi za $x = \frac{|b_0|}{4M}$. Uvrštavanjem tog izraza dobivamo $|b_0| < \frac{1}{2}|b_0|$ iz čega slijedi da je $b_0 = 0$ što je u kontradikciji s pretpostavkom da je $b_0 = a_m \neq 0$.

□

Napomena 1.2. *Prethodni teorem vrijedi i na $\mathbb{Z}[x], \mathbb{Q}[x]$ i $\mathbb{C}[x]$. Razlika je u dokazivanju za $\mathbb{Z}[x]$ jer ne postoje $x \in \mathbb{Z}$ takvi da je $x \in \langle 0, \frac{1}{2}\rangle$. Tada imamo:*

$$|b_0| = |b_1x + \cdots + b_px^p| = |x|\underbrace{|b_1 + \cdots + b_px^{p-1}|}_{\in\mathbb{Z}}, \quad x \in \mathbb{Z}.$$

Dakle, za svaki $x \in \mathbb{Z}$ vrijedi da je $|b_0|$ djeljiv s $|x|$ pa iz toga slijedi da je $b_0 = 0$.

Teorem o jednakosti polinoma dokazat ćemo koristeći Teorem o nul-polinomu.

Teorem 1.2. (O jednakosti polinoma) *(Vidjeti [1, Teorem 7.8]) Polinomi $p(x) = \sum_{i=0}^{n} a_ix^i$ i $q(x) = \sum_{i=0}^{m} b_ix^i$ za koje vrijedi $m, n \in \mathbb{N}_0$, $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in \mathbb{R}$, $a_n \neq 0, b_m \neq 0$ su jednaki ako i samo ako vrijedi $m = n$ i $a_i = b_i$, $i = 0, 1, \ldots n$.*

Dokaz.

$\Leftarrow$ Ako je $m = n$ i $a_i = b_i$ za sve $i = 0, 1, \ldots n$, onda je očito $p(x) = q(x)$, $\forall x \in \mathbb{R}$.

$\Rightarrow$ Obratno, pretpostavimo da je je $p = q$. Tada je $p - q$ nul polinom i vrijedi da je $m = n$, $a_i = b_i$ za sve $i = 0, 1, \ldots n$.
Pretpostavimo suprotno, odnosno $n \neq m$ i neka je bez smanjenja općenitosti $n > m$. Tada vrijedi:

$$(p - q)(x) = a_nx^n + \cdots + a_{m+1}x^{m+1} + (a_m - b_m)x^m + \cdots + (a_0 - b_0) = 0, \quad x \in \mathbb{R}.$$

Prema Teoremu o nul-polinomu dobivamo da je $a_n = a_{n-1} = \cdots = a_{m+1} = 0$, $a_m = b_m$, $a_{m-1} = b_{m-1}, \ldots, a_1 = b_1, a_0 = b_0$, što je u kontradikciji s pretpostavkom da je

$a_n \neq 0$. Dakle, dokazali smo da je $m = n$. Preostaje još pokazati da su $a_i = b_i$ za sve $i = 0, 1, \ldots n$. Imamo

$$(p - q)(x) = (a_n - b_n)x^n + \cdots + (a_0 - b_0) = 0$$

iz čega po Teoremu o nul-polinomu slijedi da je $a_i = b_i$ za sve $i = 0, 1, \ldots n$.

□

Primjer 1.4. *Odredite* $p(x) \in \mathbb{R}$, *ako je* $p(x + 3) = x^3 + 4x^2 - 3$.

Zbog teorema o jednakosti polinomima, slijedi da polinom $p(x)$ mora biti stupnja 3. To znači da postoje $a, b, c, d \in \mathbb{R}$ takvi da je

$$p(x) = ax^3 + bx^2 + cx + d.$$

Dalje dobivamo sljedeće:

$$\begin{aligned} p(x+3) &= a(x+3)^3 + b(x+3)^2 + c(x+3) + d \\ &= a(x^3 + 9x^2 + 27x + 27) + b(x^2 + 6x + 9) + c(x+3) + d \\ &= ax^3 + (9a + b)x^2 + (27a + 6b + c)x + 27a + 9b + 3c + d \end{aligned}$$

Po teoremu o jednakosti polinoma izjednačavamo koeficijente pa slijedi:

$$\begin{aligned} a &= 1 \\ 9a + b = 4 &\Rightarrow b = -5 \\ 27a + 6b + c = 0 &\Rightarrow c = 3 \\ 27a + 9b + 3c + d = -3 &\Rightarrow d = 6 \end{aligned}$$

Dakle, traženi polinom je $p(x) = x^3 - 5x^2 + 3x + 6$.

2 Djeljivost polinoma

Do sada smo u prstenu polinoma uveli zbrajanje i množenje, a sada ćemo uvesti pojam djeljivosti polinoma. Proučit ćemo kada je jedan polinom djeljiv drugim i opisati postupak dijeljenja dvaju polinoma te pripadna svojstva dobivenog ostatka. Sljedeća definicija i teorem preuzeti su iz [1].

Definicija 2.1. *Polinom $p \in \mathbb{R}[x]$ je **djeljiv** polinomom $q \in \mathbb{R} \setminus \{0\}$ ako postoji polinom $r \in \mathbb{R}[x]$ takav da je* st $r > 0$ *i* $p = qr$.

Teorem 2.1. (O dijeljenju s ostatkom) *(Vidjeti [1, Teorem 7.11]) Neka su $p, q \in \mathbb{R}[x]$, $q \neq 0$. Tada postoje jedinstveni polinomi $k, l \in \mathbb{R}[x]$ takvi da je $p = qk + l$, pri čemu je $l = 0$ ili* $0 \leq$ st $l <$ st q.

Dokaz. Da bi dokazali prethodni teorem, potrebno je dokazati egzistenciju i jedinstvenost polinoma k i l s traženim svojstvima.
Dokažimo prvo egzistenciju. Razlikujemo dva slučaja:
1. slučaj st $p <$ st q

U ovom slučaju jednakost $p = qk + l$ zadovoljavaju samo polinomi $k = 0$ i $l = p$ pa je očito da vrijedi da je st $l <$ st q.
2. slučaj st $p \geq$ st q

Tvrdnju dokažimo indukcijom po st p.

Ako je st $p = 0$ onda slijedi da je i st $q = 0$. Iz toga slijedi da su p i q konstantni polinomi. Dakle, jednakost $p = qk + l$ zadovoljavaju polinomi $k = \frac{p}{q}$ i $l = 0$.

Neka je st $p = m$ i $p(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,\ a_m \neq 0$. Tada definiramo $k := \frac{a_m}{b_m}$ i

$$\begin{aligned} l(x) : &= p(x) - \frac{a_m}{b_m} q(x) \\ &= (a_m x^m + \cdots + a_0) - \frac{a_m}{b_m}(b_m x^m + \cdots + b_0) \\ &= (a_{m-1} - \frac{a_m}{b_m} b_{m-1})x^{m-1} + \cdots + (a_0 - \frac{a_m}{b_m} b_0). \end{aligned}$$

Slijedi da je st $l <$ st $m =$ st q i $p = qk + l$. Time je dokazana baza indukcije.

Pretpostavimo da postoje polinomi l i k takvi da je st $l <$ st q i da vrijedi $p = qk + l$. Zapišimo polinome p i q na sljedeći način:

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_n \neq 0$$

$$q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,\ b_m \neq 0$$

i neka je $n \geq m$.
Definirajmo polinom $\overline{p}$:

$$\begin{aligned} \overline{p}(x) &= p(x) - \frac{a_n}{b_m} x^{n-m} q(x) \\ &= (a_n x^n + \cdots + a_1 x + a_0) - \frac{a_n}{b_m} x^{n-m}(b_m x^m + \cdots + b_1 x + b_0) \\ &= (a_{n-1} - \frac{a_n}{b_m} b_{m-1})x^{n-1} + \cdots + (a_{n-m} - \frac{a_n}{b_m} b_0 + a_{n-m-1}x^{n-m-1} + \cdots + a_0). \end{aligned}$$

Iz ovoga slijedi da je st $\overline{p} \leq n-1$. Ako na polinom $\overline{p}$ primijenimo pretpostavku, postoje polinomi $\overline{k}$ i $\overline{l}$, st $\overline{l} <$ st q, takvi da je

$$q(x) \cdot \overline{k}(x) + \overline{l}(x) = \overline{p}(x) = p(x) - \frac{a_n}{b_m} x^{n-m} q(x).$$

Odavdje slijedi da je

$$p(x) = q(x) \cdot (\overline{k}(x) + \frac{a_n}{b_m} x^{n-m}) + \overline{l}(x).$$

Vidimo da polinomi

$$k(x) = \overline{k}(x) + \frac{a_n}{b_m} x^{n-m}$$

i

$$l(x) = \overline{l}(x)$$

zadovoljavaju jednakost $p(x) = q(x)k(x) + l(x)$ pri čemu je st $l <$ st q i time smo dokazali egzistenciju.

Dokažimo i jedinstvenost.

Pretpostavimo da za dane polinome p i q postoje polinomi k, l, k_1, l_1 takvi da za svaki $x \in \mathbb{R}$ vrijedi

$$p(x) = q(x)k(x) + l(x)$$

uz $l = 0$ ili st $l <$ st q i

$$p(x) = q(x)k_1(x) + l_1(x)$$

uz $l_1 = 0$ ili st $l_1 <$ st q. Oduzimanjem tih jednakosti slijedi

$$q(x)(k(x) - k_1(x)) + (l(x) - l_1(x)) = 0.$$

Vidimo da, ako je

$$l(x) - l_1(x) = 0,$$

to znači da je i

$$q(x)(k(x) - k_1(x)) = 0, \quad \forall x \in \mathbb{R}.$$

Kako je $q(x) \neq 0$, slijedi da je i

$$k(x) - k_1(x) = 0$$

pa iz toga slijedi jedinstvenost.
Analogno, ako je

$$k(x) - k_1(x) = 0,$$

slijedi da je

$$l(x) - l_1(x) = 0.$$

Pretpostavimo da je $k(x) - k_1(x) \neq 0$ i $l(x) - l_1(x) \neq 0$. Tada po Propoziciji 1.1 imamo

$$\begin{aligned} \text{st } q &\leq \text{st } q + \text{st } (k - k_1) \\ &= \text{st } q(k - k_1) \\ &= \text{st } (l - l_1) \\ &\leq \max\{\text{st } l, \text{st } l_1\} \\ &< \text{st } q. \end{aligned}$$

Slijedi da je st $q <$ st q što je kontradikcija, pa smo time dokazali da je

$$k(x) = k_1(x),$$

a iz toga slijedi da je

$$l(x) = l_1(x).$$

Dakle, slijedi jedinstvenost. □

Ako je $l \neq 0$ onda polinom k zovemo **nepotpuni kvocijent** polinoma p i q, a polinom l **ostatak** pri dijeljenju polinoma p sa q.

Ako je $l = 0$ onda polinom k zovemo **kvocijent** polinoma p i q. Tada kažemo da je p **djeljiv** sa q i pišemo $q \mid p$.

Napomena 2.1. *Prethodni teorem vrijedi i za $\mathbb{Q}[x]$ i $\mathbb{C}[x]$, ali ne i za $\mathbb{Z}[x]$ jer ako su $p, q \in \mathbb{Z}[x]$ ne mora značiti da će i k, l biti u skupu $\mathbb{Z}[x]$.*

Primjer 2.1. *Koliki je ostatak pri dijeljenju polinoma $p(x) = x^{2022} - 2x + 5$ polinomom $q(x) = x^2 - 1$?*

Po prethodnom teoremu postoje jedinstveni polinomi k, l takvi da je $p = qk + l$, st $l <$ st q. Slijedi da je st $l < 2$ pa je l oblika $l(x) = ax + b$. Imamo

$$\begin{aligned} p(x) &= q(x)k(x) + ax + b \\ &= (x^2 - 1)k(x) + ax + b \end{aligned}$$

Uvrštavanjem $x = 1$ i $x = -1$ dobivamo

$$\begin{aligned} x = 1 &\Rightarrow a + b = 4 \\ x = -1 &\Rightarrow -a + b = 8 \end{aligned}$$

Iz toga slijedi da je $a = -2$ i $b = 6$, odnosno $l(x) = -2x + 6$.

Primjer 2.2. *Podijelite polinom $p(x) = x^5 - 2x^4 - 4x^3 + x^2 + x - 3$ polinomom $q(x) = x^2 - 2x + 1$.*

Postupak dijeljenja polinoma provodi se slično kao i dijeljenje cijelih brojeva. Razlikuje se jedino u tome što u ovom postupku osim brojeva imamo i varijable.

$$\begin{array}{rrrr} \big(& x^5 - 2x^4 - 4x^3 & + x^2 & + x - 3 \big) \div \big(x^2 - 2x + 1\big) = x^3 - 5x - 9 + \dfrac{-12x + 6}{x^2 - 2x + 1} \\ & -x^5 + 2x^4 & - x^3 & \\ \hline & & -5x^3 & + x^2 + x \\ & & 5x^3 & - 10x^2 + 5x \\ \hline & & & -9x^2 + 6x - 3 \\ & & & 9x^2 - 18x + 9 \\ \hline & & & -12x + 6 \end{array}$$

Vidimo da je kvocijent pri dijeljenju polinoma p sa q jednak $x^3 - 5x - 9$ dok je ostatak $-12x + 6$.

2.1 Hornerov algoritam

Hornerov algoritam nam omogućava dijeljenje polinoma linearnim polinomom $q(x) = x - \alpha$. Također je koristan i za izračunavanje vrijednosti polinoma u nekoj točki te se koristi i u numeričkoj matematici.

Neka je

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ x \in \mathbb{R},\ a_n \neq 0$$

i

$$q(x) = x - \alpha.$$

Prema Teoremu o dijeljenju s ostatkom, postoji jedinstveni polinom $k(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$ i konstanta $l \in \mathbb{R}$ (jer je $l = 0$ ili st $l = 0 <$ st q).
Uvrštavanjem dobivamo

$$\begin{aligned} a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 &= (x-\alpha)(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0) \\ &= b_{n-1}x^n + (b_{n-2} - \alpha b_{n-1})x^{n-1} + \cdots + (b_0 - \alpha b_1)x + \\ &\quad +(l - \alpha b_0). \end{aligned}$$

Po Teoremu o jednakosti polinoma vrijedi

$$\begin{aligned} a_n &= b_{n-1}, \\ a_{n-1} &= b_{n-2} - \alpha b_{n-1}, \\ a_{n-2} &= b_{n-3} - \alpha b_{n-2}, \\ &\cdots \\ a_1 &= b_0 - \alpha b_1, \\ a_0 &= l - \alpha b_0, \end{aligned}$$

te iz dobivenog računamo koeficijente polinoma k i konstantu l,

$$\begin{aligned} b_{n-1} &= a_n, \\ b_{n-2} &= a_{n-1} + \alpha b_{n-1}, \\ b_{n-3} &= a_{n-2} + \alpha b_{n-2}, \\ &\cdots \\ b_0 &= a_1 + \alpha b_1, \\ l &= a_0 + \alpha b_0. \end{aligned}$$

Na dobivenim formulama se temelji Hornerov algoritam. On se može prikazati kao u Tablici 2.1 tako da u prvi redak upišemo redom koeficijente polinoma p, a na prvo mjesto drugog retka upišemo slobodni član polinoma $q(x) = x - \alpha$ sa suprotnim predznakom. Na drugo mjesto upisujemo a_n, a na sljedeće α pomnožimo s $a_n = b_{n-1}$ i dodamo a_{n-1}. Time smo dobili b_{n-2}. Zatim dobiveni b_{n-2} množimo s α i umnošku dodajemo a_{n-2}. Time smo dobili b_{n-3}. Postupak nastavljamo sve dok ne dobijemo konstantu l koju zapisujemo ispod a_0.

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_1	a_0
α	$\underbrace{a_n}_{b_{n-1}}$	$\underbrace{a_{n-1}+\alpha b_{n-1}}_{b_{n-2}}$	$\underbrace{a_{n-2}+\alpha b_{n-2}}_{b_{n-3}}$	$\cdots$	$\underbrace{a_1+\alpha b_1}_{b_0}$	$\underbrace{a_0+\alpha b_0}_{l}$

Tablica 2.1: Hornerov algoritam

Više o Hornerovom algoritmu može se naći u [8], a sljedeći primjer prikazuje dijeljenje polinoma pomoću Hornerova algoritma.

Primjer 2.3. *Hornerovim algoritmom podijelite polinom* $p(x) = 5x^4 - 2x^3 + x^2 - 3x + 1$ *polinomom* $q(x) = x - 4$ *i izračunajte* $p(4)$.

Dakle, imamo

	5	-2	1	-3	1
4	5	18	73	289	1157

pa iz tablice možemo iščitati da vrijedi

$$p(x) = (x - 4)(5x^3 + 18x^2 + 73x + 289) + 1157.$$

Vidimo da iz dane jednakosti za $x = 4$ dobivamo $p(4) = 1157$. Iz toga zaključujemo da Hornerov algoritam možemo koristiti za računanje vrijednosti polinoma u točki α jer vrijedi da je $p(\alpha) = l$.

2.2 Najveća zajednička mjera

U ovom potpoglavlju navest ćemo definiciju i teorem o zajedničkoj mjeri polinoma te algoritam za njeno računanje koji se mogu pronaći u [1] i [6]. Nakon toga, na primjerima ćemo pokazati nalaženje najveće zajedničke mjere polinoma.

Definicija 2.2. ***Najveća zajednička mjera*** *polinoma $p, q \in \mathbb{R}[x] \setminus \{0\}$ je normirani polinom $d \in \mathbb{R}[x] \setminus \{0\}$ takav da su p i q djeljivi sa d. Pišemo $d = M(p, q)$.*

Teorem 2.2. (O najvećoj zajednjičkoj mjeri) *(Vidjeti [1, Teorem 7.18]) Za sve polinome $p, q \in \mathbb{R}[x] \setminus \{0\}$ postoji jedinstvena najveća zajednička mjera.*

Dokaz. Dokažimo prvo egzistenciju koristeći **Euklidov algoritam**. On se sastoji od uzastopne primjene Teorema o dijeljenju s ostatkom.

Pretpostavimo da je $\text{st}\, p \geq \text{st}\, q$. Prema Teoremu o dijeljenju s ostatkom postoje jedinstveni polinomi k_1 i l_1 takvi da je

$$p = qk_1 + l_1, \ \text{st}\, l_1 < \text{st}\, q.$$

Sada taj teorem primijenimo na polinome q i l_1 pa dobivamo da postoje jedinstveni polinomi k_2 i l_2 takvi da je

$$q = l_1k_2 + l_2, \ \text{st}\, l_2 < \text{st}\, l_1.$$

U sljedećem koraku dobivamo da postoje k_3 i l_3 takvi da je

$$l_1 = l_2k_3 + l_3, \ \text{st}\, l_3 < \text{st}\, l_2.$$

Primjenjujući dalje ovaj postupak dolazimo do niza ostataka $l_1, l_2, l_3, \ldots$ čiji stupnjevi strogo padaju pa jednom dolazimo do ostatka $l_i \neq 0$ tako da je u sljedećem koraku,

$$l_{i-1} = l_ik_{i+1} + l_{i+1},$$

ostatak $l_{i+1} = 0$. Iz posljednje dobivene jednakosti vidimo da l_i dijeli l_{i-1} pa iz toga dalje slijedi da l_i dijeli l_{i-2} i tako dalje. Zatim dolazimo do druge jednakosti gdje zaključujemo da l_i dijeli q i do prve gdje l_i dijeli p. Dakle, l_i dijeli polinome p i q.

Neka je $a_n \neq 0$ vodeći koeficijent polinoma l_i. Tada normiranjem polinoma l_i dobivamo normirani polinom

$$d = \frac{1}{a_n} l_i$$

takav da d dijeli p i q.

Potrebno je još dokazati da je d polinom najvećeg stupnja koji dijeli p i q. Neka je $s \in \mathbb{R}[x]$ takav da dijeli polinome p i q. Iz prve jednakosti slijedi $l_1 = p - qk_1$ pa s dijeli l_1. Iz druge jednakosti slijedi $l_2 = q - l_1k_2$ pa s dijeli i l_2. Analogno nastavljajući postupak zaključujemo da s dijeli i l_i, odnosno d. Dakle, d je najveća zajednička mjera polinoma p i q.

Nakon egzistencije, dokažimo i jedinstvenost.
Neka je $s \in \mathbb{R}[x]$ najveća zajednička mjera. Tada vrijedi da je $\text{st}\, s = \text{st}\, d$. Već smo pokazali da s dijeli d. Slijedi da postoji $r \in \mathbb{R}[x]$ takav da je $d = rs$. Kako znamo da su d i s normirani polinomi, po Teoremu o jednakosti polinoma vrijedi da je $r = 1$, tj. $d = s$. □

Definicija 2.3. *Ako za $p, q \in \mathbb{R}[x]$ vrijedi da je $M(p, q) = 1$ onda kažemo da su polinomi p i q* ***relativno prosti****.*

Napomena 2.2. *Dokaz prethodnog teorema daje nam spomenuti Euklidov algoritam koji se sastoji od toga da, ukoliko je* st $p \geq$ st q*, prvo podijelimo p sa q. Tada dobivamo ostatak l_1 te q dijelimo sa l_1 i dobivamo ostatak l_2. Zatim l_1 dijelimo sa l_2 i dobivamo l_3. Postupak nastavljamo dok ne dođemo do prvog l_i takvog da je $l_{i+1} = 0$. Normirani l_i je tada najveća zajednička mjera polinoma p i q.*

Primjer 2.4. *Neka su $p, q \in \mathbb{R}[x]$ takvi da je $p(x) = -2x^4 - 2x^3 + 6x^2 + 8x + 2$ i $q(x) = -2x^3 - 2x^2 + 2x + 2$. Odredite $M(p, q)$.*

Za početak je potrebno podijeliti polinome p i q.

$$\begin{array}{l} \big(-2x^4 - 2x^3 + 6x^2 + 8x + 2\big) \div \big(-2x^3 - 2x^2 + 2x + 2\big) = x + \dfrac{4x^2 + 6x + 2}{-2x^3 - 2x^2 + 2x + 2} \\ \underline{\;\; 2x^4 + 2x^3 - 2x^2 - 2x \;\;} \\ \qquad\qquad 4x^2 + 6x + 2 \end{array}$$

Vidimo da je ostatak pri dijeljenju $l_1 = 4x^2 + 6x + 2$. Sada je potrebno polinom q podijeliti polinomom l_1:

$$\begin{array}{l} \big(-2x^3 - 2x^2 + 2x + 2\big) \div \big(4x^2 + 6x + 2\big) = -\frac{1}{2}x + \frac{1}{4} + \dfrac{\frac{3}{2}x + \frac{3}{2}}{4x^2 + 6x + 2} \\ \underline{\;\; 2x^3 + 3x^2 + x \;\;} \\ \qquad\qquad x^2 + 3x + 2 \\ \qquad\qquad \underline{-x^2 - \frac{3}{2}x - \frac{1}{2}} \\ \qquad\qquad\qquad \frac{3}{2}x + \frac{3}{2} \end{array}$$

Dobili smo ostatak $l_2 = \frac{3}{2}x + \frac{3}{2}$ pa dijelimo l_1 sa l_2:

$$\begin{array}{l} \big(4x^2 + 6x + 2\big) \div \big(\frac{3}{2}x + \frac{3}{2}\big) = \frac{8}{3}x + \frac{4}{3} \\ \underline{-4x^2 - 4x} \\ \qquad\quad 2x + 2 \\ \qquad\quad \underline{-2x - 2} \\ \qquad\qquad 0 \end{array}$$

Vidimo da smo posljednjim dijeljenjem dobili da je ostatak jednak 0. Dakle, potrebno je normirati polinom l_2 da bi dobili najveću zajedničku mjeru. Dijeljenem l_2 sa $\frac{3}{2}$ dobivamo da je $M(p, q) = x + 1$.

Primjer 2.5. *Neka su $p, q \in \mathbb{R}[x]$ takvi da je $p(x) = 2x^3 - 5x^2 + 9x - 9$ i $q(x) = x^2 - x + 3$. Odredite $M(p, q)$.*

Dijeljenjem polinoma p i q dobivamo:

$$\begin{array}{l} \big(2x^3 - 5x^2 + 9x - 9\big) \div \big(x^2 - x + 3\big) = 2x - 3 \\ \underline{-2x^3 + 2x^2 - 6x} \\ \qquad\quad -3x^2 + 3x - 9 \\ \qquad\quad \underline{3x^2 - 3x + 9} \\ \qquad\qquad 0 \end{array}$$

Vidimo da polinom q dijeli poliom p pa je $M(p, q) = q = x^2 - x + 3$.

3 Nultočke polinoma

Dosad smo proučavali polinome iz skupa $\mathbb{R}[x]$, ali ista svojstva vrijede i za polinome iz $\mathbb{C}[x]$, pa ćemo odsad promatrati polinome iz prstena $\mathbb{C}[x]$. U ovom poglavlju navest ćemo definicije i teoreme vezane uz nultočke polinoma, algebarske jednadžbe i traženje rješenja algebarskih jednadžbi.

Definicija 3.1. ***Nultočka polinoma*** $f \in \mathbb{C}[x]$ *je kompleksan broj* $\alpha \in \mathbb{C}$ *za koji vrijedi* $f(\alpha) = 0$.

Napomena 3.1. *Ako je* $\alpha \in \mathbb{R}$ *onda kažemo da je* α *realna nultočka.*

Iskažimo i dokažimo Bézoutov teorem za polinome.

Teorem 3.1. (Bézoutov teorem za polinome) *(Vidjeti [1, Teorem 7.22])* α *je nultočka polinoma* $p \in \mathbb{C}[x]$ *ako i samo ako je* p *djeljiv polinomom* $q(x) = x - \alpha$.

Dokaz.

$\Rightarrow$ Neka je α nultočka polinoma p, tj. $f(\alpha) = 0$. Po Teoremu o dijeljenju s ostatkom postoje $k \in \mathbb{R}[x]$ i $l \in \mathbb{C}$ takvi da je

$$p(x) = (x - \alpha)k(x) + l.$$

Uvrštavanjem $x = \alpha$ dobivamo $p(\alpha) = l$, a kako znamo da je $p(\alpha) = 0$ slijedi da je $l = 0$. Dakle, polinom $q = x - \alpha$ dijeli polinom p.

$\Leftarrow$ Pretpostavimo da je polinom p djeljiv polinomom $q = x - \alpha$. To znači da postoji $k \in \mathbb{C}$ takav da je $p(x) = (x - \alpha)k(x)$. Uvrštavanjem $x = \alpha$ dobivamo da je $p(\alpha) = 0$ što znači da je α nultočka od p.

□

Definicija 3.2. *Ako je* $p \in \mathbb{C}[x]$ *djeljiv polinomom* $(x-\alpha)^r$, *ali nije djeljiv sa* $(x-\alpha)^{r+1}$, *za neki* $\alpha \in \mathbb{C}$ *i* $r \in \mathbb{N}$ *onda kažemo da je* α r***-struka nultočka*** *od* p *ili nultočka* ***kratnosti*** r.

Određivanje kratnosti nultočke prikazat ćemo sljedećim primjerom.

Primjer 3.1. *Odredite kratnost nultočke* $x = -3$ *polinoma* $p(x) = x^4 + 7x^3 + 13x^2 - 3x - 18$.

Podijelimo p sa $(x + 3)$ koristeći Hornerov algoritam:

	1	7	13	-3	-18
-3	1	4	1	-6	0

Dakle, $p(x) = (x + 3)(x^3 + 4x^2 + x - 6)$ pa ponovno koristimo Hornerov algoritam:

	1	4	1	-6
-3	1	1	-2	0

Iz toga slijedi da je $p(x) = (x + 3)^2(x^2 + x - 2) = (x + 3)^2 k(x)$. Kako je $k(-3) \neq 0$ onda po Bézoutovom teoremu slijedi da $(x + 3)$ ne dijeli polinom k pa je $x = 3$ dvostruka nultočka od p.

3.1 Faktorizacija polinoma

Da bi iskazali i dokazali teorem o faktorizaciji polinoma nad $\mathbb{C}$ potreban nam je Osnovni teorem algebre čiji dokaz se može pronaći u [9], a ostale tvrdnje koje ćemo navoditi mogu se pronaći u [1] i [6].

Teorem 3.2. (Osnovni teorem algebre) *(Vidjeti [1, Teorem 7.25]) Neka je* $p \in \mathbb{C}[x]$, st $p \geq 1$. *Tada postoji* $\alpha \in \mathbb{C}$ *takav da je* $p(\alpha) = 0$.

Napomena 3.2. *Prethodni teorem ne vrijedi na* $\mathbb{R}[x]$ *jer polinomi s realnim koeficijentima ne moraju imati realnu nultočku. Na primjer, polinom* $p(x) = x^2 + 2$ *nema realnu nultočku. Zato kažemo da je polje* $\mathbb{C}$ *algebarski zatvoreno, a* $\mathbb{Q}, \mathbb{Z}$ *i* $\mathbb{R}$ *nisu algebarski zatvorena polja.*

Teorem 3.3. *(Vidjeti [1, Korolar 7.26]) Svaki polinom* $p \in \mathbb{C}[x]$ *n-tog stupnja može se na jedinstven način prikazati kao produkt n polinoma prvog stupnja. Točnije, ako je* $a \in \mathbb{C}$ *vodeći koeficijent polinoma p, onda postoje* $\alpha_i \in \mathbb{C}, i = 1, 2, \ldots, n$ *takvi da*

$$p(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Dokaz. Dokažimo prvo egzistenciju koristeći matematičku indukciju po stupnju polinoma p.
Baza: Za $n = 1$ imamo

$$p(x) = a_1 x + a_0 = a_1(x - \frac{a_0}{a_1}).$$

Pretpostavka: Pretpostavimo da se za $n \in \mathbb{N}$ polinom stupnja n može prikazati kao produkt n polinoma prvog stupnja, tj.

$$p(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Korak: Neka je p polinom stupnja $n + 1$. Tada po Osnovnom teoremu algebre postoji α_{n+1} takav da je $p(\alpha_{n+1}) = 0$. Dalje, po Bézoutovom teoremu slijedi da $(x - \alpha_{n+1})$ dijeli p, odnosno postoji $k \in \mathbb{C}[x]$ takav da je

$$p(x) = (x - \alpha_{n+1})k(x), \ x \in \mathbb{C}.$$

Vrijedi da je st $k = n$ pa iz pretpostavke indukcije slijedi da postoje $\alpha_i \in \mathbb{C}, i = 1, 2, \ldots, n$ takvi da je

$$k(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Uvrštavanjem u $p(x)$ dobivamo

$$p(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)(x - \alpha_{n+1}). \tag{3.1}$$

Sada dokažimo i jedinstvenost.
Pretpostavimo da postoje $\beta_i \in \mathbb{C}, i = 1, 2, \ldots, n$ i $b \in \mathbb{C}$ takvi da je

$$p(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = b(x - \beta_1)(x - \beta_2) \cdots (x - \beta_n).$$

Po Teoremu o jednakosti polinoma vrijedi $a = b$. Ako bi neka nultočka α_i bila različita od nultočke β_j onda bi lijeva strana jednakosti bila jednaka nuli, a desna različita od nule. Iz toga slijedi da je svaki α_i jednak nekom β_j.

Treba još pokazati da se kratnosti nultočaka podudaraju.
Pretpostavimo suprotno. Neka je $\alpha_i = \beta_j$, ali α_i je r-struka nultočka dok je β_j t-struka nultočka i vrijedi $r > t$. Tada vidimo da $(x - \alpha)^r$ dijeli lijevu stranu jednakosti 3.1, a desnu ne. Analogno i pretpostavka $r < t$ vodi kontradikciji. Dakle, kratnosti se podudaraju i jedinstvenost je dokazana. □

Teorem 3.4. *(Vidjeti [6, Teorem 11]) Svaki polinom $p \in \mathbb{C}[x]$ stupnja $n \geq 1$ ima točno n nultočaka, pri čemu svaku nultočku brojimo onoliko puta kolika je njezina kratnost.*

Dokaz. Iz prethodnog torema slijedi da se svaki polinom $p \in \mathbb{C}[x]$ može zapisati u obliku

$$p(x) = a_n(x-\alpha_1)^{r_1}(x-\alpha_2)^{r_2}\cdots(x-\alpha_t)^{r_t}, \tag{3.2}$$

gdje su $\alpha_1, \alpha_2, \ldots, \alpha_t$ međusobno različite nultočke od p, a r_j kratnost nultočke α_j, $j = 1, 2, \ldots, t$. Pri tome vrijedi

$$r_1 + r_2 + \cdots + r_t = n.$$

Kada bi kratnost nultočke α_j bila jednaka c_j, tada bi vrijedilo $r_j \leq c_j$. U slučaju $r_j < c_j$ bismo imali

$$p(x) = (x-\alpha_j)^{c_j} \cdot \rho(x),$$

gdje ρ ne sadrži faktor $p_j(x) = x - \alpha_j$. Rastavljanjem polinoma ρ i uvrštavanjem u prethodnu jednakost nećemo dobiti rastav 4.1 tako da mora biti $r_j = c_j$. □

Teorem 3.5. *(Vidjeti [6, Teorem 12]) Ako su polinomi p i q stupnja koji nije veći od n i podudaraju se u barem $n+1$ točaka, onda je $p = q$.*

Dokaz. Razlika polinoma p i q čiji stupanj nije veći od n je

$$s(x) = p(x) - q(x)$$

te njegov stupanj također nije veći od n. Ako za $x_1, x_2, \ldots, x_c$, $c > n$ vrijedi

$$p(x_1) = q(x_1), p(x_2) = q(x_2), \ldots, p(x_c) = q(x_c),$$

to znači da su brojevi $x_i, i = 1, 2, \ldots, c$ nultočke polinoma s. Tada bi s imao više od n nutočaka. Dakle, h je konstantan polinom, a kako ima nultočku, on mora biti nul-polinom. □

3.2 Viète formule

U ovom potpoglavlju iskazat ćemo i dokazati teorem o Viète formulama koje nam daju vezu između nultočki i koeficijenata nekog polinoma. One nam ponekad mogu biti korisne za računanje s nultočkama polinoma kao što će biti prikazano na primjerima u nastavku.

Teorem 3.6. (Viète) *(Vidjeti [7, Teorem 3.3.1]) Neka je* $p(x) = \sum_{i=0}^{n} a_i x^n$, $a_i \in \mathbb{C}$, $a_n \neq 0$, *te neka su* $x_1, x_2, \ldots, x_n$ *njegove nultočke. Tada vrijede Viète formule:*

$$\begin{aligned}
\eta_1 &= \sum_{i=1}^{n} x_i = -\frac{a_{n-1}}{a_n}, \\
\eta_2 &= \sum_{1\leq i<j\leq n} x_i x_j = \frac{a_{n-2}}{a_n}, \\
\eta_3 &= \sum_{1\leq i<j<k\leq n} x_i x_j x_k = -\frac{a_{n-3}}{a_n}, \\
&\cdots \\
\eta_n &= \prod_{i=1}^{n} x_i = (-1)^n \frac{a_0}{a_n}.
\end{aligned}$$

Dokaz. Dokaz ćemo provesti koristeći matematičku indukciju.

Baza: Za $n = 1$ imamo polinom prvog stupnja $p(x) = a_1 x + a_0$. Neka je x_1 njegova nultočka. Tada je $x_1 = -\frac{a_0}{a_1}$. Iz toga slijedi da tvrdnja vrijedi za $n = 1$.

Pretpostavka: Pretpostavimo da Viète formule vrijede za polinom $p \in \mathbb{C}[x]$ stupnja n. Neka je p oblika

$$p(x) = b_n x^n + b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_1 x + b_0,$$

pri čemu su $x_1, x_2, \ldots, x_n$ njegove nultočke. Tada vrijedi

$$\begin{aligned}
\eta_1 &= -\frac{b_{n-1}}{b_n}, \\
\eta_2 &= \frac{b_{n-2}}{b_n}, \\
\eta_3 &= -\frac{b_{n-3}}{b_n}, \\
&\cdots \\
\eta_k &= (-1)^k \frac{b_{n-k}}{b_n}, \\
&\cdots \\
\eta_n &= (-1)^n \frac{b_0}{b_n}.
\end{aligned}$$

Korak: Dokažimo da Viète formule vrijede i za polinom $p \in \mathbb{C}[x]$ čiji stupanj je jednak $n + 1$.

$$p(x) = a_{n+1} x^{n+1} + a_n x^n + \cdots + a_1 x + a_0,$$

pri čemu su $x_1, x_2, \ldots, x_n, x_{n+1}$ nultočke polinoma p. Prema Osnovnom teoremu algebre slijedi da polinom p ima barem jednu nultočku x_{n+1}. Dalje, po Bézoutovom teoremu, polinom

p je djeljiv s $x-x_{n+1}$ pa postoje $b_0, b_1, \ldots, b_n$ takvi da polinom p možemo zapisati na sljedeći način

$$p(x) = (x - x_{n+1})(b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0).$$

Uvrštavanjem $p(x)$ dobivamo

$$a_{n+1}x^{n+1} + a_n x^n + \cdots + a_1 x + a_0 = (x - x_{n+1})(b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0).$$

Po Teoremu o jednakosti polinoma slijedi

$$\begin{aligned} b_n &= a_{n+1}, \\ b_{n-1} &= a_n + b_n x_{n+1}, \\ &\cdots \\ b_{n-k} &= a_{n-k+1} + b_{n-k+1}x_{n+1}, \\ &\cdots \\ b_0 &= -\frac{a_0}{x_{n+1}}. \end{aligned}$$

Iz tako dobivenih jednakosti i pretpostavke indukcije slijedi

$$\begin{aligned} x_1 + x_2 + \cdots + x_{n+1} &= \eta_1 + x_{n+1} \\ &= -\frac{b_{n-1}}{b_n} + x_{n+1} \\ &= -\frac{a_n + a_{n+1}x_{n+1}}{a_{n+1}} + x_{n+1} \\ &= -\frac{a_n}{a_{n+1}} \\ &\cdots \\ x_1x_2\cdots x_k + x_{n-k+1}\cdots x_k &+ \cdots + x_{n-k+2}\cdots x_n x_{n+1} = \\ &= \eta_k + x_{n+1}\eta_{k-1} \\ &= (-1)^{k+1}\cdot\frac{b_{n-k}}{b_n} + (-1)^k \cdot \frac{b_{n-k+1}}{b_n}x_{n+1} \\ &= \frac{(-1)^{k+1}(a_{n-k+1} + b_{n-k+1}x_{n+1}) + (-1)^k x_{n+1}b_{n-k+1}}{b_n} \\ &= (-1)^{k+1}\cdot\frac{a_{n-k+1}}{a_{n+1}} \\ &\cdots \\ x_1x_2\cdots x_{n+1} &= \eta_n x_{n+1} \\ &= (-1)^n \cdot \frac{b_0}{b_n}x_{n+1} \\ &= (-1)^n \cdot \frac{\frac{-a_0}{x_{n+1}}}{a_{n+1}}x_{n+1} \\ &= (-1)^{n+1}\cdot\frac{a_0}{a_{n+1}} \end{aligned}$$

Dakle, Vièteove formule vrijede za polinom bilo kojeg stupnja. □

U sljedećim primjerima pokazat ćemo kada je moguće koristiti Vièteove formule i kako nam to olakšava rješavanje nekih zadataka. Na taj način ne moramo računati nultočke polinoma, ali pomoću njih znamo koliko iznose izrazi koji sadrže nultočke polinoma.

Primjer 3.2. *Neka su x_1, x_2 nultočke polinoma $p(x) = 3x^2 + 4x + 1$. Izračunajte $x_1 + x_2$ i $x_1 \cdot x_2$ bez određivanja nultočki polinoma.*

Vidimo da se radi o polinomu stupnja 2 pa je $a_2 = 3, a_1 = 4, a_0 = 1$. Tada, koristeći Viètеove formule imamo

$$\begin{aligned} x_1 + x_2 &= -\frac{a_1}{a_2} = -\frac{4}{3} \\ x_1 \cdot x_2 &= (-1)^2 \cdot \frac{a_0}{a_2} = \frac{1}{3} \end{aligned}$$

Primjer 3.3. *Neka su x_1, x_2, x_3 nultočke polinoma $p(x) = 5x^3 + x^2 - 3x + 2$. Izračunajte $\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$ bez određivanja nultočki polinoma.*

Raspisivanjem traženog zbroja imamo

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = \frac{x_2x_3 + x_1x_3 + x_1x_2}{x_1x_2x_3}$$

te vidimo da za računanje brojnika trebamo koristiti formulu η_2 za $n = 3$, a u nazivniku formulu η_3 iz Viètеovih formula. Pri tome vrijedi da je $a_3 = 5, a_2 = 1, a_1 = -3, a_0 = 2$. Tada imamo

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = \frac{x_2x_3 + x_1x_3 + x_1x_2}{x_1x_2x_3} = \frac{\frac{a_1}{a_3}}{(-1)^3 \cdot \frac{a_0}{a_n}} = \frac{\frac{-3}{5}}{-\frac{2}{5}} = \frac{3}{2}.$$

Primjer 3.4. *Neka su x_1, x_2 nultočke polinoma $p(x) = 6x^2 - 2x + 12$. Izračunajte $x_1^3x_2^2 + x_1^2x_2^3$ bez određivanja nultočki polinoma.*

Raspišimo dani izraz kako bismo mogli koristiti Viètеove formule.

$$x_1^3x_2^2 + x_1^2x_2^3 = x_1^2x_2^2(x_1 + x_2) = (x_1x_2)^2(x_1 + x_2)$$

Vidimo da je $a_2 = 6, a_1 = -2, a_0 = 12$ pa vrijedi

$$\begin{aligned} x_1 \cdot x_2 &= \frac{a_0}{a_2} = \frac{12}{6} = 2 \\ x_1 + x_2 &= -\frac{a_1}{a_2} = -\frac{-2}{6} = \frac{1}{3}. \end{aligned}$$

Uvrštavanjem u traženi izraz dobivamo

$$x_1^3x_2^2 + x_1^2x_2^3 = 2^2 \cdot \frac{1}{3} = \frac{4}{3}.$$

4 Algebarske jednadžbe

Da bismo mogli navoditi svojstva algebarskih jednadžbi za početak ćemo navesti definiciju algebarske jednadžbe koja je preuzeta iz [1].

Definicija 4.1. *Jednadžbu oblika*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0, \tag{4.1}$$

gdje su $n \in \mathbb{N}$, $a_0, a_1, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, *zovemo* ***algebarska jednadžba*** n***-tog stupnja.***
Ako je $a_n = 1$ *onda za jednadžbu kažemo da je* ***normirana.***
Broj x_0 *zovemo* ***korijen*** *ili* ***rješenje jednadžbe*** *4.1 ako vrijedi*

$$a_n x_0^n + a_{n-1} x_0^{n-1} + \cdots + a_1 x_0 + a_0 = 0.$$

Jednadžbi 4.1 pridružujemo polinom $p(x) = \sum_{i=0}^{n} a_i x^i$.
Svako rješenje jednadžbe je nultočka pripadnog polinoma.
Kažemo da je x_0 r***-struki korijen*** *od 4.1 ako je* x_0 r*-struka nultočka od* p.

Kako smo Teoremom 3.4 dokazali da svaki polinom n-tog stupnja ima točno n nultočki, tako jednadžba 4.1 ima n rješenja, pri čemu svako rješenje brojimo onoliko puta kolika mu je kratnost. No, vidimo da nam Teorem ne daje metodu za nalaženje rješenja neke jednadžbe.

Proučavanjem algebarskih jednadžbi ovog tipa matematičari se bave još od oko 2000. godine prije Krista u egipatskoj i babilonskoj matematici. Jednadžbe prvog stupnja (linearne jednadžbe) spominju se u najstarijim matematičkim izvorima - Rhindovom i Moskovskom papirusu. U njima se nalaze zadaci koji su uglavnom posvećeni rješavanju praktičnih problema koji se svode na rješavanje linearnih jednadžbi. Rješenje takvih jednadžbi je trivijalno, tj. ako je $a_1 x + a_0 = 0$ onda je rješenje dano sa $x_0 = -\frac{a_0}{a_1}$.

Za razliku od egipatske, babilonska matematika je bila naprednija jer su znali rješavati neke jednadžbe drugog stupnja (kvadratne jednadžbe) i trećeg stupnja (kubne jednadžbe). Svoje zapise zapisivali su na glinenim pločicama te se tako na njima našla tablica rješenja jednadžbi $x^2(x \pm 1) = a$ za različite a. Linearne i kvadratne jednadžbe proučavale su se i u antičkoj Grčkoj, ali su problemu pristupali geometrijski koristeći konstruktivne metode. Nalaženje rješenja kvadratnih jednadžbi nije trivijalno, ali prvu općenitu metodu za njihovo rješavanje dao je indijski matematičar Brahmagupta u obliku formule izražene riječima.

Formule za rješenja jednadžbi trećeg i četvrtog stupnja poznate su od 16. stoljeća. Tada je formulu za rješenje opće jednadžbe trećeg stupnja otkrio talijanski matematičar Gerolamo Cardano, a formulu za rješenje jednadžbe četvrtog stupnja njegov učenik Lodovico Ferrari.

Nakon tih saznanja nametalo se pitanje postoje li formule za nalaženje rješenja jednadžbe stupnja većeg od 4. Tek početkom 19.stoljeća, norveški matematičar Niels Henrik Abel dokazuje da za opću jednadžbu petog stupnja ili više ne postoji algebarsko rješenje. Dakle, rješenje takvih jednadžbi ne možemo pronaći koristeći algebarske operacije (zbrajanje, oduzimanje, množenje, dijeljenje) i potencije s racionalnim eksponentima.

4.1 Cjelobrojna rješenja algebarske jednadžbe

U ovom potpoglavlju spomenut ćemo neka svojstva cjelobrojnih rješenja algebarske jednadžbe. Za početak je iskazan i dokazan teorem koji nam govori kako odrediti cjelobrojna rješenja, ako postoje, jednadžbe s cjelobrojnim koeficijentima.

Teorem 4.1. *(Vidjeti [1, Propozicija 7.31]) Neka je dana jednadžba* $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, *gdje su* $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, *te* $\alpha \in \mathbb{Z} \setminus \{0\}$ *rješenje jednadžbe. Tada* α *dijeli slobodni član* a_0.

Dokaz. Kako je α korijen algebarske jednadžbe, tada vrijedi

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Iz toga dobivamo

$$a_0 = -\alpha(a_n\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_2\alpha + a_1).$$

Izraz unutar zagrade nalazi se u skupu $\mathbb{Z}$, pa iz toga slijedi da α dijeli a_0. □

Prethodni teorem nam olakšava traženje rješenja algebarskih jednadžbi pa pokažimo sada na primjeru kako je moguće pomoću njega pronaći cjelobrojna rješenja jednadžbe, ukoliko postoje.

Primjer 4.1. *Riješite jednadžbu* $x^4 + x^3 - 8x^2 - 2x + 12 = 0$.

Po prethodnom teoremu, ukoliko algebarska jednadžba ima cjelobrojna rješenja, ona su djelitelji slobodnog člana. Dakle, kandidati za cjelobrojna rješenja su:

$$-1, 1, -2, 2, -3, 3, -4, 4, -6, 6, -12, 12.$$

Neka je $p(x) = x^4 + x^3 - 8x^2 - 2x + 12$ polinom pridružen danoj algebarskoj jednadžbi. Provjerimo redom dobivene kandidate:

$$p(-1) = 6,\ p(1) = 4,\ p(-2) = -8,\ p(2) = 0,\ p(-3) = 0,\ p(3) = 42,\ p(-4) = 84,\ p(4) = 196,$$

$$p(-6) = 816,\ p(6) = 1224,\ p(-12) = 17892,\ p(12) = 21300.$$

Vidimo da su $\alpha_1 = 2$ i $\alpha_2 = -3$ cjelobrojne nultočke polinoma p. Po Bézoutovom teoremu slijedi da polinomi $(x-2)$ i $(x+3)$ dijele polinom p.

Podijelimo polinome koristeći Hornerov algoritam:

	1	1	-8	-2	12
2	1	3	-2	-6	0
-3	1	0	-2	0	

Dakle, $p(x) = (x-2)(x+3)\underbrace{(x^2-2)}_{q(x)}$, pa su preostala rješenja jednadžbe nultočke polinoma q, tj. $\alpha_3 = \sqrt{2}$ i $\alpha_4 = -\sqrt{2}$.

U Primjeru 4.1 vidimo da je slobodni član imao mnogo djelitelja, pa smo za mnogo brojeva ispitivali jesu li oni rješenja jednadžbe. Korištenjem sljedećeg teorema možemo skratiti taj postupak.

Teorem 4.2. *(Vidjeti [6, Teorem 14]) Neka je dana jednadžba* $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, *gdje su* $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, *te* $\alpha \in \mathbb{Z} \setminus \{0\}$ *rješenje jednadžbe. Tada je za svaki* $k \in \mathbb{Z}$ *broj* $\alpha - k$ *djelitelj od* $p(k)$ *gdje je* p *polinom pridružen danoj algebarskoj jednadžbi.*

Dokaz. α je rješenje algebarske jednadžbe pa vrijedi

$$p(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Nadalje,

$$p(k) = a_n k^n + a_{n-1}k^{n-1} + \cdots + a_1 k + a_0.$$

Oduzimanjem ovih dviju jednakosti dobivamo:

$$-p(k) = a_n(\alpha^n - k^n) + a_{n-1}(\alpha^{n-1} - k^{n-1}) + \cdots + a_1(\alpha - k).$$

Vidimo da je svaki od binoma s desne strane jednakosti djeljiv s $\alpha - k$, pa zaključujemo da je i lijeva strana jednakosti djeljiva s $\alpha - k$. Dakle, p(k) je djeljiv s $\alpha - k$. □

Riješimo sada sljedeći primjer koristeći prethodni teorem.

Primjer 4.2. *Riješite jednadžbu* $x^3 - 8x^2 + 25x - 26 = 0$.

Kako je cjelobrojni koeficijent $a_0 = -26$, to znači da su kandidati za cjelobrojna rješenja brojevi

$$\alpha \in \{1, -1, 2, -2, 6, -6, 13, -13, 26, -26\}.$$

Neka je $p(x) = x^3 - 8x^2 + 25x - 26$ polinom pridružen danoj algebarskoj jednadžbi. Uzmimo da je $k = 1$, tada je $p(k) = p(1) = -8$. Vidimo da broj 1 nije nultočka ovog polinoma.

Tada je

$$(\alpha - k) = (\alpha - 1) \in \{0, -2, 1, -3, 5, -7, 12, -14, 25, -27\}.$$

Kako je $p(1) = -8$, on nije djeljiv s 0, -3, 5, 7, 12, -14, 25 i -27, po prethodnom teoremu, α nije jedan od brojeva 1, -2, 6, -6, 16, -13, 26 i -26.

Tada nam kao kandidati za cjelobrojne nultočke ostaju samo brojevi -1 i 2. Kako je $p(-1) = -60$, a $p(2) = 0$, to znači da je $\alpha_1 = 2$ jedina cjelobrojna nultočka i vrijedi

$$p(x) = (x - 2)(x^2 - 6x + 3).$$

Ostale nultočke su $\alpha_2 = 3 - 2i$ i $\alpha_3 = 3 + 2i$.

4.2 Racionalna rješenja algebarske jednadžbe

Nakon što smo pokazali kako je moguće pronaći cjelobrojna rješenja algebarske jednadžbe, pokazat ćemo kako se određuju racionalna rješenja algebarske jednadžbe s cjelobrojnim koeficijentima. O tome nam govori sljedeći teorem.

Teorem 4.3. *(Vidjeti [1, Teorem 7.34]) Neka je dana jednadžba* $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, *gdje su* $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, *te* $a_n \neq 0$. *Ako je* $\alpha = \frac{f}{g}$, $f \in \mathbb{Z}$, $g \in \mathbb{N}$, $M(f,g) = 1$, *rješenje dane jednadžbe, onda* f *dijeli slobodni član* a_0, *a* g *dijeli vodeći koeficijent* a_n.

Dokaz. Kako znamo da je $\alpha = \frac{f}{g}$ rješenje jednadžbe, onda vrijedi

$$a_n \left(\frac{f}{g}\right)^n + a_{n-1}\left(\frac{f}{g}\right)^{n-1} + \cdots + a_1 \frac{f}{g} + a_0 = 0.$$

Sada dobivenu jednakost množimo sa g^n i dobivamo:

$$a_n f^n + a_{n-1} f^{n-1} g + \cdots + a_1 f g^{n-1} + a_0 g^n = 0. \tag{4.2}$$

Iz 4.2 slijedi

$$a_0 g^n = -f(a_n f^{n-1} + a_{n-1} f^{n-2} g + \cdots + a_2 f g^{n-2} + a_1 g^{n-1}),$$

pa vidimo da f dijeli $a_0 g^n$. Kako po pretpostavci teorema znamo da je najveća zajednička mjera brojeva f i g jednaka 1, znači da f može dijeliti samo a_0. Također, iz 4.2 slijedi

$$a_n f^n = -g(a_0 g^{n-1} + a_1 g^{n-2} f + \cdots + a_{n-2} g f^{n-2} + a_{n-1} f^{n-1}).$$

Dakle, g dijeli $a_n f^n$ te analogno zaključujemo da onda mora vrijediti da g dijeli a_n. □

Riješimo sljedeći primjer koristeći prethodni teorem.

Primjer 4.3. *Riješite jednadžbu* $3x^2 - 8x - 3 = 0$.

Po prethodnom teoremu imamo:

$$f \in \{1, -1, 3, -3\}, \quad g \in \{1, 3\}.$$

Ako dana jednadžba ima racionalno rješenje onda vrijedi

$$\frac{f}{g} \in \left\{1, -1, 3, -3, \frac{1}{3}, -\frac{1}{3}\right\}.$$

Neka je $p(x) = 3x^2 - 8x - 3$ polinom pridružen danoj algebarskoj jednadžbi. Tada imamo

$$p(1) = -8,\ p(-1) = 8,\ p(3) = 0,\ p(-3) = 48,\ p\left(\frac{1}{3}\right) = -\frac{16}{3},\ p\left(-\frac{1}{3}\right) = 0.$$

Dakle, $\alpha_1 = 3$ i $\alpha_2 = -\frac{1}{3}$ su rješenja dane jednadžbe.

Ako slobodni član i vodeći koeficijent imaju mnogo djelitelja onda postupak traženja rješenja na ovaj način može biti kompliciran. Primjenom sljedećeg teorema možemo skratiti taj postupak što će biti prikazano u primjeru nakon.

Teorem 4.4. *(Vidjeti [6, Teorem 16]) Ako je* $\alpha = \frac{f}{g}$, $f \in \mathbb{Z}$, $g \in \mathbb{N}$, $M(f,g) = 1$, *racionalno rješenje jednadžbe* $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, *gdje su* $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, *onda je za svaki broj* k *broj* $f - gk$ *djelitelj od* $p(k)$ *gdje je* p *polinom pridružen polaznoj algebarskoj jednadžbi.*

Primjer 4.4. *Riješite jednadžbu* $25x^4 + 15x^3 + 16x^2 - 9x + 1 = 0$.

Po prethodnom teoremu imamo:

$$f \in \{1, -1\}, \quad g \in \{1, 5, 25\}.$$

Ako dana jednadžba ima racionalno rješenje onda vrijedi

$$\frac{f}{g} \in \left\{1, -1, \frac{1}{5}, -\frac{1}{5}, \frac{1}{25}, -\frac{1}{25}\right\}.$$

Neka je $p(x) = 25x^4 + 15x^3 + 16x^2 - 9x + 1$ polinom pridružen danoj algebarskoj jednadžbi. Uzmimo da je $k = -1$. Vrijedi $p(-1) = 36$ te tada imamo

$$f - gk = f + g \in \{2, 0, 6, -4, 26, 24\}.$$

Vidimo da 0,26 i 24 nisu djelitelji od 36 pa iz toga slijedi

$$\frac{f}{g} \in \left\{1, \frac{1}{5}, -\frac{1}{5}\right\}.$$

Uzmimo sada da je $k = 1$.
$p(1) = 48$ te imamo

$$f - gk = f - g \in \{0, -4, -6\}$$

iz čega vidimo da jedino 0 nije djelitelj od 48 pa su nam jedini kandidati za racionalne nultočke

$$\frac{f}{g} \in \left\{\frac{1}{5}, -\frac{1}{5}\right\}.$$

Uvrštavanjem u $p(x)$ dobivamo

$$f(\frac{1}{5}) = 0, \quad f(-\frac{1}{5}) = \frac{84}{25}$$

te je $\alpha_1 = \frac{1}{5}$ jedina racionalna nultočka.
Dijeljenjem f sa $(x - \frac{1}{5})$ dobivamo

$$p(x) = \left(x - \frac{1}{5}\right)(25x^3 + 20x^2 + 20x - 5).$$

Tada analogni postupak ponavljamo za jednadžbu $25x^3 + 20x^2 + 20x - 5 = 0$ te dobivamo njena rješenja:

$$\alpha_2 = \frac{1}{5}, \alpha_3 = \frac{-1 + i\sqrt{3}}{2}, \alpha_4 = \frac{-1 - i\sqrt{3}}{2}.$$

Dakle, $\alpha = \frac{1}{5}$ je dvostruko racionalno rješenje ove jednadžbe.

4.3 Kompleksna rješenja algebarske jednadžbe

Kompleksni brojevi su oblika $\alpha + \beta i$, gdje su α i β realni brojevi, a i je imaginarna jedinica. Mi ćemo u ovom potpoglavlju iskazati kako se pronalaze kompleksna rješenja algebarske jednadžbe za koje su α i β cijeli brojevi u navedenom obliku. Za početak ćemo iskazati i dokazati lemu koja će nam kasnije biti potrebna.

Lema 4.1. *(Vidjeti [1, Lema 7.37]) Neka su $a_i \in \mathbb{R}$, $i = 0, 1, \ldots, n$ te neka je $x_0 = \alpha + \beta i \in \mathbb{C}$ rješenje jednadžbe $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$. Tada je i $\overline{x_0} = \alpha - \beta i$ također rješenje pripadne jednadžbe.*

Dokaz. U ovom dokazu koristit ćemo sljedeća pravila za konjugiranje:

$$\begin{aligned} \overline{z_1 + z_2} &= \overline{z_1} + \overline{z_2} \\ \overline{z_1 z_2} &= \overline{z_1}\,\overline{z_2} \\ \overline{n} &= n \end{aligned}$$

gdje su $z_1, z_2 \in \mathbb{C}$ i $n \in \mathbb{R}$.
Neka je x_0 kompleksno rješenje jednadžbe, a p polinom pridružen danoj jednadžbi. Tada vrijedi $p(x_0) = 0$. Izračunajmo $p(\overline{x_0})$,

$$\begin{aligned} p(\overline{x_0}) &= a_n \overline{x_0}^n + a_{n-1}\overline{x_0}^{n-1} + \cdots + a_1\overline{x_0} + a_0 \\ &= a_n \overline{x_0^n} + a_{n-1}\overline{x_0^{n-1}} + \cdots + a_1\overline{x_0} + a_0 \\ &= \overline{a_n x_0^n} + \overline{a_{n-1}x_0^{n-1}} + \cdots + \overline{a_1 x_0} + \overline{a_0} \\ &= \overline{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{p(x_0)} \\ &= 0. \end{aligned}$$

Dakle, $\overline{x_0}$ je također rješenje jednadžbe. □

Pogledajmo sada sljedeći teorem koji nam govori o svojstvu kompleksnih rješenja algebarske jednadžbe.

Teorem 4.5. *(Vidjeti [1, Teorem 7.38]) Neka su $a_i \in \mathbb{R}$, $i = 0, 1, \ldots, n$ te neka je $x_0 = \alpha + \beta i$ rješenje jednadžbe $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, pri čemu su $\alpha, \beta \in \mathbb{Z}$. Tada je $\alpha^2 + \beta^2$ djelitelj slobodnog člana a_0.*

Dokaz. Neka je p polinom pridružen danoj jednadžbi. Po prethodnoj lemi znamo da, ako je $p(\alpha + \beta i) = 0$, onda je i $p(\alpha - \beta i) = 0$. Dalje, po Bézoutovom teoremu slijedi da je p djeljiv s $(x - (\alpha + \beta i))$ i $(x - (\alpha - \beta i))$, odnosno s polinomom

$$\begin{aligned} q(x) &= (x - (\alpha + \beta i))(x - (\alpha - \beta i)) \\ &= x^2 - 2\alpha x + \alpha^2 + \beta^2. \end{aligned} \tag{4.3}$$

Iz toga slijedi da je $p(x)$ oblika

$$\begin{aligned} p(x) &= q(x)k(x) \\ &= (x^2 - 2\alpha x + \alpha^2 + \beta^2)(b_{n-2}x^{n-2} + \cdots + b_0). \end{aligned} \tag{4.4}$$

Po Teoremu o jednakosti polinoma vidimo da za slobodni član a_0 vrijedi

$$a_0 = (\alpha^2 + \beta^2)b_0,$$

te iz toga slijedi tvrdnja. □

Napomena 4.1. *Pogledajmo izraz 4.4 i primijetimo da ga možemo zapisati i na sljedeći način:*

$$\begin{aligned} q(x) &= ((x-\alpha)+\beta i)((x-\alpha)-\beta i) \\ &= (x-\alpha)^2-(\beta i)^2 \\ &= (x-\alpha)^2+\beta^2. \end{aligned}$$

Dakle, specijalno za $x = k$ u 4.4 vidimo da $(k-\alpha)^2+\beta^2$ dijeli $p(k)$ što nam može olakšati potragu za cjelobrojnim kompleksnim nultočkama.

Primjer 4.5. *Riješite jednadžbu $x^4-4x^3+11x^2-14x+10=0$.*

Broj 10 je slobodni član ove jednadžbe, pa iz toga slijedi da je

$$(\alpha^2+\beta^2) \in \{1,2,5,10\}.$$

Prikazivajući te brojeve u obliku zbroja kvadrata dobivamo:

$$\begin{aligned} 1 &= 0^2+1^2 = 1^2+0^2 \\ 2 &= 1^2+1^2 \\ 5 &= 2^2+1^2 = 1^2+2^2 \\ 10 &= 3^2+1^2 = 1^2+3^2. \end{aligned}$$

Dakle, kandidati za kompleksna rješenja ove jednadžbe su

$$(\alpha+\beta i) \in \{\pm 1, \pm i, 1\pm i, -1\pm i, 2\pm i, -2\pm i, 1\pm 2i, -1\pm 2i, 3\pm i, -3\pm i, 1\pm 3i, -1\pm 3i\}.$$

Uzmimo $k=1$. $p(1)=4$, pa je

$$((k-\alpha)^2+\beta^2) \in \{0,2,4,5,8,9,10,13,17\}.$$

Kako 0,5,10,8,9,13 i 17 nisu djelitelji broja 4, preostaje nam da je

$$(\alpha+\beta i) \in \{-1, \pm i, 1\pm i, 2\pm i, 1\pm 2i\}.$$

Uzmimo da je sada $k=2$. $p(2)=10$, pa je

$$((k-\alpha)^2+\beta^2) \in \{1,2,5,9\}.$$

Kako 9 ne dijeli broj 10, slijedi

$$(\alpha+\beta i) \in \{\pm i, 1\pm i, 2\pm i, 1\pm 2i\}.$$

Sada imamo manje kandidata pa uvrštavanjem u danu jednadžbu dobivamo da su njena rješenja $x_{1,2}=1\pm i$ i $x_{3,4}=1\pm 2i$.

5 Reducibilni i ireducibilni polinomi

U ovom poglavlju definirat ćemo reducibilnost i ireducibilnost polinoma te iskazati i dokazati teoreme koji govore o ireducibilnosti nad $\mathbb{R}$ i $\mathbb{C}$ koji se mogu pronaći u [1] te o reducibilnosti nad $\mathbb{Q}$ koji se mogu pronaći u [6].

Definicija 5.1. *Neka je $\mathbb{P}$ neko od polja $\mathbb{R}, \mathbb{Q}$ ili $\mathbb{C}$. Polinom $p \in \mathbb{P}[x]$ je **reducibilan** nad $\mathbb{P}$ ako postoje polinomi $f, g \in \mathbb{P}[x]$,* st *$f \geq 1$,* st *$g \geq 1$, takvi da je $p = fg$. Ako p nije reducibilan onda kažemo da je **ireducibilan**.*

Napomena 5.1. *Uočavamo da reducibilnost polinoma ovisi o polju $\mathbb{P}$. Na primjer, pogledajmo polinom $p = x^2 + 4 = (x - 2i)(x + 2i)$. Očito je da je reducibilan nad $\mathbb{C}$, a ireducibilan nad $\mathbb{R}$. Razlog tomu je što p nema realnu nultočku pa se po Bézoutovom teoremu p ne može podijeliti nijednim polinomom stupnja 1.*

Teorem 5.1. *(Vidjeti [1, Teorem 7.42]) Neka je $p \in \mathbb{C}[x]$ ireducibilan. Tada je* st *$p \leq 1$.*

Dokaz. Neka je $p \in \mathbb{C}[x]$. Pretpostavimo suprotno, odnosno da je st $p \geq 2$.

Po Osnovnom teoremu algebre postoji $x_0 \in \mathbb{C}$ koji je nultočka polinoma p, tj. $p(x_0) = 0$. Dalje, po Bézoutovom teoremu slijedi da $(x - x_0)$ dijeli polinom p. Dakle, postoji $k \in \mathbb{C}[x]$, st $k \geq 1$ takav da je

$$p(x) = (x - x_0)k(x).$$

Time smo došli do kontradikcije s ireducibilnošću od p, pa je time dokazana tvrdnja. □

Napomena 5.2. *Kvadratna jednadžba nad $\mathbb{R}$ je oblika*

$$a_2x^2 + a_1x + a_0 = 0$$

gdje su $a_2, a_1a_0 \in \mathbb{R}$ i $a_2 \neq 0$. Tada vrijedi

$$\begin{aligned} 0 &= x^2 + \frac{a_1}{a_2}x + \frac{a_0}{a_2} \\ &= \left(x + \frac{a_1}{2a_2}\right)^2 - \frac{a_1^2}{4a_2^2} + \frac{a_0}{a_2} \\ &= \left(x + \frac{a_1}{2a_2}\right)^2 - \frac{a_1^2 - 4a_2a_0}{4a_2}. \end{aligned}$$

Iz toga slijedi

$$\left(x + \frac{a_1}{2a_2}\right)^2 = \frac{a_1^2 - 4a_2a_0}{4a_2}.$$

Dakle, rješenja jednadžbe su

$$x_{1,2} = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2a_0}}{2a_2}.$$

Iz ovoga zaključujemo da je polinom $p = a_2x^2 + a_1x + a_0$ ireducibilan nad $\mathbb{R}$ ako i samo ako je $a_1^2 - 4a_2a_0 < 0$.

Teorem 5.2. *(Vidjeti [1, Teorem 7.43]) Ako je $p \in \mathbb{R}[x]$ ireducibilan, onda je* st *$p \leq 2$. Svi normirani ireducibilni polinomi su oblika $1, x - a$ za $a \in \mathbb{R}$ i $x^2 + a_1x + a_0$ za $a_1, a_0 \in \mathbb{R}$ takvi da je $a_1^2 < 4a_0$.*

Dokaz. Iz prethodnog teorema i napomene je očito da su navedeni polinomi ireducibilni. Potrebno je još dokazati da su svi ireducibilni polinomi iz $\mathbb{R}[x]$ tog oblika.

Neka je $p \in \mathbb{R}[x]$. Pretpostavimo da je st $p \geq 3$. Vidimo da je $p \in \mathbb{C}[x]$, pa po Osnovnom teoremu algebre postoji $x_0 \in \mathbb{C}$ koji je nultočka polinoma p, tj. $p(x_0) = 0$. Tada postoje dvije mogućnosti.

a) $x_0 \in \mathbb{R}$
Tada po Bézoutovom teoremu slijedi da $(x - x_0)$ dijeli polinom p. On je tada oblika

$$p(x) = (x - x_0)k(x),$$

gdje je $k \in \mathbb{R}[x]$ i st $k \geq 2$. Iz toga slijedi da je p reducibilan.

b) $x_0 \in \mathbb{C} \setminus \mathbb{R}$
$x_0 = \alpha + \beta i$, pri čemu su $\alpha, \beta \in \mathbb{R}, \beta \neq 0$. Prema Lemi 4.1 je i $\overline{x_0} = \alpha - \beta i$ nultočka polinoma p. Dakle, polinom p možemo faktorizirati na sljedeći način

$$\begin{aligned} p(x) &= (x - x_0)(x - \overline{x_0})k(x) \\ &= \underbrace{(x^2 - 2\alpha x + \alpha^2 + \beta^2)}_{\in \mathbb{R}[x]} k(x), \end{aligned}$$

pa je p reducibilan.

□

Teorem 5.3. *(Vidjeti [6, Teorem 19]) Ako je $p \in \mathbb{Q}[x]$, st $p = 2$, onda je p reducibilan ako i samo ako ima barem jednu racionalnu nultočku.*

Dokaz. Neka je $p(x) = a_2x^2 + a_1x + a_0$, $a_2 \neq 0$ i x_1 racionalna nultočka polinoma p. Iz Viètеovih formula slijedi da je tada i druga nultočka, x_2, racionalna. Dakle, p možemo faktorizirati na sljedeći način:

$$p(x) = a_2(x - x_1)(x - x_2),$$

pa zaključujemo da je p reducibilan.

Obrnuto, neka je $p \in \mathbb{Q}[x]$ reducibilan. Tada je oblika

$$p(x) = (ax + b)(cx + d),$$

gdje su $a, c \neq 0$, $a, b, c, d \in \mathbb{Q}$. Dakle, $x_1 = -\frac{b}{a}$ i $x_2 = -\frac{d}{c}$ su racionalne nultočke polinoma p. □

Teorem 5.4. *(Vidjeti [6, Teorem 20]) Polinom $p \in \mathbb{Q}[x]$, st $p = 3$, reducibilan je ako i samo ako ima barem jednu racionalnu nultočku.*

Dokaz. Neka je $p \in \mathbb{Q}[x]$ takav da je st $p = 3$. Ako p ima racionalnu nultočku $x_0 = \frac{f}{g}$, gdje je $f \in \mathbb{Z}$, $g \in \mathbb{N}$, onda p možemo rastaviti u obliku

$$p(x) = \left(x - \frac{f}{g}\right) k(x).$$

Iz Euklidovog algortima slijedi da je $k \in \mathbb{Q}[x]$. Dakle, p je reducibilan.

Obrnuto, neka je $p \in \mathbb{Q}[x]$ reducibilan. Tada je oblika

$$p(x) = (ax + b)(cx^2 + dx + e),$$

gdje su $a, c \neq 0$, $a, b, c, d, e \in \mathbb{Q}$. Vidimo da je $x_0 = -\frac{b}{a}$ racionalna nultočka polinoma p. □

Primjer 5.1. *Ispitajte je li polinom* $p(x) = 10x^3 - 19x^2 + 62x - 8$ *reducibilan nad* $\mathbb{Q}$.

Prema prethodnom teoremu, dovoljno je provjeriti ima li polinom p racionalnu nultočku. Koristeći opisani postupak traženja racionalnih rješenja algebarske jednadžbe dobivamo da je $x_1 = \frac{2}{5}$ racionalna nultočka polinoma p. Dakle, p možemo rastaviti na sljedeći način

$$p(x) = (5x - 2)(2x^2 - 3x + 4).$$

Iz toga slijedi da je p reducibilan nad $\mathbb{Q}$.

6 Derivacija polinoma

Polinom je funkcija, a derivacije funkcija općenito se definiraju analitički, koristeći limes. No, derivacije polinoma mogu se definirati algebarski kao što će biti prikazano u nastavku.

Definicija 6.1. *Neka je* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$, $a_i \in \mathbb{R}$, $i = 0, 1, 2, \ldots, n$ *polinom.* ***Derivacija polinoma*** p *je polinom* p' *definiran kao*

$$p'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

p' *nazivamo još i* ***prva derivacija*** *ili* ***derivacija prvog reda****.*

Primjer 6.1. *Odredite prvu derivaciju polinoma* $p(x) = 4x^3 + 3x^2 + 5x + 6$.

Iz definicije vidimo da je potrebno stupanj svakog člana pomnožiti s koeficijentom te stupanj smanjiti za jedan. Dakle, imamo

$$\begin{aligned} p'(x) &= 4 \cdot 3x^{3-1} + 3 \cdot 2x^{2-1} + 5x^{1-1} \\ &= 12x^2 + 6x + 5. \end{aligned}$$

Napomena 6.1. *Vidimo da, ukoliko deriviramo polinom* p *koji je* n*-tog stupnja, dobit ćemo polinom* p' $(n-1)$*-vog stupnja. Dakle, i prva derivacija ima derivaciju. Nju nazivamo* ***druga derivacija*** *ili* ***derivacija drugog stupnja****. Postupak možemo nastaviti do* n*-te derivacije*

$$p^{(n)}(x) = (p^{(n-1)}(x))'.$$

Primjer 6.2. *Odredite derivacije polinoma* $p(x) = 2x^5 + x^4 + 3x^3 + x^2 + 8$.

Vrijedi

$$\begin{aligned} p'(x) &= 10x^4 + 4x^3 + 9x^2 + 8x, \\ p''(x) &= 40x^3 + 12x^2 + 18x + 8, \\ p'''(x) &= 120x^2 + 24x + 18, \\ p^{(4)}(x) &= 240x + 24, \\ p^{(5)}(x) &= 240, \\ p^{(6)}(x) &= p^{(7)}(x) = \cdots = 0. \end{aligned}$$

Iskažimo i dokažimo svojstva derivacije polinoma koja se mogu pronaći u [6].

Teorem 6.1. *Neka su* p *i* q *polinomi. Tada vrijedi*

$$\begin{aligned} (\alpha p + \beta q)'(x) &= \alpha p'(x) + \beta q'(x), \quad \forall \alpha, \beta \in \mathbb{R},\ p, q \in \mathbb{R}[x], \\ (pq)'(x) &= p'(x) \cdot q(x) + p(x) \cdot q'(x), \quad p, q \in \mathbb{R}[x], \\ (p^r)' &= r \cdot p^{r-1} \cdot p', \forall r \in \mathbb{N},\ p \in \mathbb{R}[x], \end{aligned}$$

gdje je p^r *produkt* $p \cdot p \cdots p$ *od* r *faktora.*

Dokaz. Neka su

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0, \\ q(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0, \end{aligned}$$

gdje su $a_i, b_j \in \mathbb{R}$, $i = 0, 1, \ldots, n$, $j = 0, 1, \ldots, m$. Dokažimo prvo svojstvo. Pretpostavimo da je $n \geq m$. Tada, za $\alpha, \beta \in \mathbb{R}$, imamo

$$(\alpha p + \beta q)(x) = \alpha a_n x^n + \alpha a_{n-1} x^{n-1} + \cdots + (\alpha a_m + \beta b_m) x^m + \cdots (\alpha a_1 + \beta b_1) x + (\alpha a_0 + \beta b_0).$$

Derivirajmo pripadni izraz prema definiciji derivacije.

$$\begin{aligned} (\alpha p + \beta q)'(x) &= n\alpha a_n x^{n-1} + (n-1)\alpha a_{n-1} x^{n-2} + \cdots + \\ &+ m(\alpha a_m + \beta b_m) x^{m-1} + \cdots + (\alpha a_1 + \beta b_1). \end{aligned}$$

S druge strane,

$$\begin{aligned} \alpha p'(x) + \beta q'(x) &= \alpha(n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1) + \\ &+ \beta(m b_m x^{m-1} + (m-1) b_{m-1} x^{m-2} + \cdots + b_1). \end{aligned}$$

Sređivanjem dobivenog izraza imamo

$$\alpha p'(x) + \beta q'(x) = n\alpha a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + (\alpha a_1 + \beta b_1).$$

Dakle, prvo svojstvo je dokazano.

Dokažimo sada drugo svojstvo. Proučit ćemo tri slučaja:

1. Ako imamo dane funkcije $p(x) = x^n$ i $q(x) = x^m$, onda vrijedi

   $$p'(x) = n x^{n-1}, \quad q'(x) = m x^{m-1}.$$

   Dakle, dobivamo

   $$\begin{aligned} p'(x) \cdot q(x) + p(x) \cdot q'(x) &= n x^{n-1} x^m + x^n m x^{m-1} \\ &= (n+m) x^{n+m-1}. \end{aligned}$$

   Derivirajmo sada izraz $(pq)(x) = x^{n+m}$:

   $$(pq)'(x) = (n+m) x^{n+m-1}.$$

   Iz toga dobivamo

   $$p'(x) \cdot q(x) + p(x) \cdot q'(x) = (pq)'(x),$$

   pa zaključujemo da za ovaj slučaj vrijedi drugo svojstvo.

2. Neka je $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ i $q(x) = x^m$. Sada je

   $$\begin{aligned} (pq)'(x) &= (a_n x^{n+m} + \cdots + a_1 x^{m+1} + a_0 x^m)' \\ &= (n+m) a_n x^{n+m-1} + \cdots + (m+1) a_1 x^m + m a_0 x^{m-1} \\ &= m(a_n x^n + \cdots + a_1 x + a_0) x^{m-1} + (n a_n x^{n-1} + \cdots + 2a_2 x + a_1) x^m \\ &= p(x) \cdot q'(x) + p'(x) \cdot q(x), \end{aligned}$$

   pa drugo svojstvo vrijedi i za ovaj slučaj.

3. Neka je
$$p(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$
i
$$q(x) = b_m x^m + \cdots + b_2 x^2 + b_1 x + b_0.$$
Tada vrijedi
$$(pq)(x) = b_m x^m p(x) + \cdots + b_1 x p(x) + b_0 p(x).$$
Iz prvog svojstva i prva dva slučaja slijedi
$$\begin{aligned}(pq)'(x) &= mb_m x^{m-1} p(x) + \cdots + 2b_2 x p(x) + b_1 p(x) + \\ &+ b_m x^m p'(x) + \cdots + b_1 x p'(x) + b_0 p'(x) \\ &= p(x)(mb_m x^{m-1} + \cdots + 2b_2 x + b_1) + p'(x)(b_m x^m + \cdots + b_1 x + b_0) \\ &= p(x) \cdot q'(x) + p'(x) \cdot q(x),\end{aligned}$$
pa je time dokazano drugo svojstvo.

Treće svojstvo dokazat ćemo indukcijom. Primijetimo da, ukoliko u drugom svojstvu stavimo $p = q$, onda dobivamo
$$\begin{aligned}(p^2)' &= p \cdot p' + p' \cdot p \\ &= 2p \cdot p',\end{aligned}$$
a to je upravo treće svojstvo za $r = 2$.

Pretpostavimo da svojstvo vrijedi za prirodni broj r, odnosno
$$(p^r)' = r \cdot p^{r-1} \cdot p'.$$
Imamo
$$\begin{aligned}(p^{r+1})' &= (p^r \cdot p)' \\ &= (p^r)' \cdot p + p^r \cdot p' \\ &= r \cdot p^{r-1} \cdot p' \cdot p + p^r \cdot p' \\ &= r \cdot p^r \cdot p' + p^r \cdot p' \\ &= (r+1) \cdot p^r \cdot p'\end{aligned}$$
i time je dokazano i treće svojstvo. □

Primjenu ovih svojstava pokazat ćemo na primjerima u nastavku.

Primjer 6.3. *Derivirajte polinom* $p(x) = (x^3 + 4x^2)(7x^2 + 2x + 3)$.

Vidimo da je u ovom primjeru moguće primijeniti drugo svojstvo, pa imamo
$$\begin{aligned}p'(x) &= (x^3 + 4x^2)' \cdot (7x^2 + 2x + 3) + (x^3 + 4x^2) \cdot (7x^2 + 2x + 3)' \\ &= (3x^2 + 12x) \cdot (7x^2 + 2x + 3) + (x^3 + 4x^2) \cdot (14x + 2) \\ &= 35x^4 + 120x^3 + 33x^2 + 24x\end{aligned}$$

Primjer 6.4. *Derivirajte polinom* $p(x) = (x^2+1)^2(5x+6)$.

U ovom primjeru ćemo koristiti drugo i treće svojstvo. Dakle, imamo

$$\begin{aligned} p'(x) &= 2\cdot(x^2+1)\cdot(x^2+1)'\cdot(5x+6) + (x^2+1)^2\cdot(5x+6)' \\ &= 2\cdot(x^2+1)\cdot(2x)\cdot(5x+6) + (x^2+1)^2\cdot(5x) \\ &= 25x^4 + 24x^3 + 30x^2 + 24x + 5. \end{aligned}$$

Sljedeći teorem govori nam o vezi nultočke polinoma i njegove derivacije.

Teorem 6.2. *(Vidjeti [6, Teorem 6]) Ako je* α *nultočka polinoma* p *kratnosti* $r \geq 2$*, onda je* α *nultočka prve derivacije polinoma* p*, i to kratnosti* $r-1$.

Dokaz. Ako je α nultočka polinoma p, onda znamo da ga možemo zapisati u sljedećem obliku

$$p(x) = (x-\alpha)^r k(x),$$

pri čemu je $k(x)$ polinom koji nije djeljiv s $(x-\alpha)$, $k(\alpha) = 0$. Deriviranjem polinoma p dobivamo

$$\begin{aligned} p'(x) &= r(x-\alpha)^{r-1}k(x) + (x-\alpha)^r k'(x) \\ &= (x-\alpha)^{r-1}[rk(x) + (x-\alpha)k'(x)] \end{aligned}$$

iz čega vidimo da je α nultočka od p', kratnosti $r-1$. □

Literatura

[1] Z. Bujanović, B. Muha, *Elementarna matematika 1*, Prirodoslovno matematički fakultet-Matematički odsjek, Zagreb, 2017.

[2] F. M. Brückler: *Povijest matematike I*, Sveučilište J. J. Strossmayera u Osijeku, Odjel za matematiku, 2007.

[3] F. M. Brückler: *Povijest matematike II*, Sveučilište J. J. Strossmayera u Osijeku, Odjel za matematiku, 2010.

[4] T. W. Hungerford, *Algebra, Graduate Texts in Mathematics vol. 73*, 2003.

[5] J. Janković, *Prsteni polinoma i formalnih redova*, Prirodoslovno matematički fakultet-Matematički odsjek, Sveučilište u Zagrebu, Zagreb, Diplomski rad, 2018.

[6] B. Pavković, D. Veljan, *Elementarna matematika I*, Tehnička knjiga, Zagreb, 1992.

[7] I. Purgar, *Polinomi*, Prirodoslovno matematički fakultet- Matematički odsjek, Sveučilište u Zagrebu, Zagreb, Diplomski rad, 2018.

[8] Z. Tomljanović, *Hornerov algoritam i primjene*, Osječki matematički list, **7** (2007), 99–106

[9] Š. Ungar, *Matematička analiza 4*, skripta, 2001., `https://web.math.pmf.unizg.hr/~ungar/NASTAVA/MA/Analiza4.pdf`

Sažetak

U ovom radu proučavani su polinomi u jednoj varijabli. Nakon njihova definiranja, prikazane su računske operacije s polinomima te je dokazano da skup svih polinoma čini prsten. Zatim je, pomoću Teorema o nul-polinomu, dokazan i Teorem o jednakosti polinoma. Opisano je kada su polinomi djeljivi i Hornerov algoritam za dijeljenje polinoma linearnim polinomom. Definirana je najveća zajednička mjera dvaju polinoma te je Euklidovim algoritmom prikazan postupak traženja iste. Proučavane su i nultočke polinoma, njihova svojstva i faktorizacija polinoma nakon koje je dokazan Viètеov teorem. Potom su definirane algebarske jednadžbe i objašnjeni su postupci traženja cjelobrojnih, racionalnih i kompleksnih rješenja. Za kraj, definirana je reducibilnost i ireducibilnost polinoma te derivacija polinoma i njihova svojstva.

Ključne riječi: polinomi, Hornerov algoritam, Euklidov algoritam, Viètеov teorem, algebarske jednadžbe, reducibilnost, derivacija polinoma

Polynomials in one variable

Summary

In this work, polynomials in one variable were studied. After defining them, computational operations with polynomials were presented and it was proved that the set of all polynomials forms a ring. Then, using the Zero polynomial theorem, the Theorem of polynomial equality was also proved. It is described when polynomials are divisible and Horner's algorithm for dividing a polynomial by a linear polynomial is given. The largest common measure of two polynomials is defined, and the procedure for finding it using the Euclidean algorithm is presented. Zeros of polynomials, their properties and factorization of polynomials were also studied, afterwards Viète's theorem was proved. Algebraic equations are then defined and the procedures of searching for integer, rational and complex solutions are explained. Finally, the reducibility and irreducibility of polynomials and the derivation of polynomials and their properties are defined.

Keywords: polynomials, Horner's algorithm, Euclid's algorithm, Viète's theorem, algebraic equations, reducibility, polynomial derivation

Životopis

Rođena sam u Osijeku, 14.03.1997. godine. Pohađala sam osnovnu školu "Mladost" u Osijeku od 2003. godine, a njenim završetkom upisala sam I.gimnaziju u Osijeku. Nakon završene srednje škole upisala sam Preddiplomski sveučilišni studij matematike na Odjelu za matematiku Sveučilišta J.J. Strossmayera u Osijeku. Stjecanjem prvostupničke diplome, 2020. godine upisujem diplomski Nastavnički studij matematike i informatike na istom fakultetu. Za vrijeme studiranja dvije godine sam radila kao asistent u nastavi.