Polinomi in njihove ničle [1]

Emil Žagar

2. junij 2012

[1]Skripta je v nastajanju, zato je gotovo polna napak. Hvaležen bom za vse pripombe. Iskanje napak je obenem del učnega procesa pri Proseminarju B.

Kazalo

1 Uvod **5**
1.1 Formalna konstrukcija polinomov 5
1.2 Evklidov algoritem 7
1.3 Ničle polinomov 9

2 Kompleksni polinomi **13**
2.1 Osnovni izrek algebre 13
2.2 Descartesovo pravilo predznakov 17

3 Dodatek **25**

Poglavje 1

Uvod

Polinomi so ena najpomembnejših matematičnih struktur nasploh. Brez njih računalniki ne bi bili sposobni izračunati praktično ničesar. Kljub temu, da jih ponavadi uvedemo zaradi računskih potreb, jih lahko definiramo tudi zelo formalno, kot algebraično strukturo. V nadaljevanju bomo privzeli, da je množica $A \neq \{0\}$, opremljena z adicijo multiplikacijo, celostno polje, torej komutativen kolobar z enoto brez deliteljev niča. Nekateri rezultati veljajo tudi v primeru, ko je A samo kolobar, a tega ne bomo posebej izpostavljali. Nekateri rezultati pa bodo res samo za polja, torej komutativne obsege, a bomo to posebej poudarili. V primerih bo A ponavadi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ali $\mathbb{C}$.

1.1 Formalna konstrukcija polinomov

V tem razdelku bomo definirali polinome kot zaporedja s končno mnogo od nič različnimi elementi (glejte na primer [2]). Na njih bomo definirali operaciji seštevanja in množenja, kar bo porodilo strukturo kolobarja.
Naj bo $\mathcal{S}$ množica zaporedij s končnim nosilcem, torej

$$\mathcal{S} = \{(a_0, a_1, a_2, \dots);\ a_i \in A,\ i = 0, 1, \dots\},$$

pri čemer je v vsakem zaporedju samo končno mnogo elementov a_i različnih od 0 (z 0 bomo označevali tako nevtralni element za seštevanje v A, kot tudi 0 kot naravno število). Obstaja torej $n \in \mathbb{N}$ (k naravnim številom štejemo tudi 0), da je $a_j = 0$ za vsak $j \geq n$. Množico $\mathcal{S}$ opremimo z operacijama seštevanja $+$ in množenja $\cdot$.

Definicija 1.1. *Za $P = (a_0, a_1, \dots)$ in $Q = (b_0, b_1, \dots)$ iz $\mathcal{S}$ naj bo*

$$\begin{aligned} P + Q &= (a_0 + b_0, a_1 + b_1, \dots), \\ P \cdot Q &= (a_0\, b_0, a_0\, b_1 + a_1\, b_0, \dots, a_0\, b_i + a_1\, b_{i-1} + \dots + a_i\, b_0, \dots). \end{aligned}$$

Iz zgornje definicije je očitno, kako seštejemo dva polinoma. Postopek je enak, kot bi seštevali dva vektorja v končnodimenzionalnem prostoru (ne pozabimo, da imajo zaporedja samo končno mnogo neničelnih elementov). Množenje je malce bolj zapleteno. Seveda ga poznamo že iz srednje šole, kjer smo se srečali s klasičnimi polinomi. Kot temu radi rečemo, množimo "vsakega z vsakim". Tu pa si na kratko oglejmo, kako lahko množenje izvedemo malo bolj formalno.
Naj bosta $P, Q \in \mathcal{S}$ in $R = P \cdot Q$. Označimo $R = (c_0, c_1, \dots, c_i, \dots)$. Najprej opazimo, da je $R \in \mathcal{S}$, saj ima končno mnogo neničelnih elementov. Torej je množenje dobro definirano. Oglejmo si definicijo elementa $c_i = a_0\, b_i + a_1\, b_{i-1} + \cdots + a_i\, b_0$. Če definiramo $\boldsymbol{a}_i = (a_0, a_1, \dots, a_i)$ in $\boldsymbol{b}_i = (b_0, b_1, \dots, b_i)$ ter $\mathrm{fliplr}(\boldsymbol{a}_i) = (a_i, a_{i-1}, \dots, a_1, a_0)$, potem je

$$c_i = \mathrm{fliplr}(\boldsymbol{a}_i) .\cdot \boldsymbol{b}_i, \quad i = 0, 1, \dots$$

Pri tem $.\cdot$ pomeni množenje po komponentah[1], torej za vektorja $\boldsymbol{c}_i = (c_0, c_1, \dots, c_i)$ in $\boldsymbol{d}_i = (d_0, d_1, \dots, d_i)$ velja

$$\boldsymbol{c}_i .\cdot \boldsymbol{d}_i = c_0 \cdot d_0 + c_1 \cdot d_1 + \cdots + c_i \cdot d_i.$$

Struktura $(\mathcal{S}, +, \cdot)$ je *kolobar polinomov* nad kolobarjem koeficinetov A (dokaz je preprost, zahtevnejši bralec naj ga izdela sam). Poseben pomen ima element $X = (0, 1, 0, \dots)$, saj je

$$X^k = (\underbrace{0, 0, \dots, 0}_{k-\text{krat}}, 1, 0, \dots), \quad k \in \mathbb{N}.$$

Elementu X rečemo spremenljivka ali nedoločenka nad A. Če nadalje element $a_i \in A$ identificiramo z elementom $(a_i, 0, \dots) \in \mathcal{S}$, lahko polinom $P = (a_0, a_1, \dots)$ zapišemo kot

$$P = a_0 + a_1\, X + a_2\, X^2 + \cdots + a_n\, X^n.$$

Kolobar polinomov $(\mathcal{S}, +, \cdot)$ označimo z $A[X]$.

Definicija 1.2. *Naj bo $P = (a_0, a_1, \dots) \in A[X]$. Če je $a_i = 0$ za vsak $i \in \mathbb{N}$, polinomu P rečemo ničelni polinom in pišemo $P = 0$. Če $P \neq 0$, naj bo $n \in \mathbb{N}$ največje naravno število, za katerega je $a_n \neq 0$. Potem je $n = \deg(P)$ stopnja polinoma P (pri tem definiramo $\deg(0) = -\infty$). Koeficinetu a_n rečemo vodilni koeficient polinoma P, členu $a_n\, X^n$ pa vodilni člen polinoma P. Če je $a_n = 1$ (kjer je 1 enota kolobarja A), potem polinomu P rečemo monični polinom.*

[1] Množenje po komponentah je denimo zelo značilna operacija v programskem paketu Matlab (kaj več o Matlabu lahko izveste v [4]).

Za vodilni koeficient in vodilni člen bomo uporabljali oznaki $\mathrm{lc}(P)$ in $\mathrm{lt}(P)$.

Primer 1.1. *Naj bo* $A = \mathbb{Z}$ *in* $P = (1, 2, 0, 1, 0, \dots)$ *ter* $Q = (1, -1, 0, \dots)$. *Potem je* $P = 1 + 2\,X + X^3$, $Q = 1 - X$, $P + Q = 2 + X + X^3$ *in* $P \cdot Q = 1 + X - 2\,X^2 + X^3 - X^4$. *Stopnja polinoma* P *je* $\deg(P) = 3$, *njegov vodilni koeficinet* $\mathrm{lc}(P) = 1$, *vodilni člen polinoma* Q *pa je* $\mathrm{lt}(Q) = -X$.

Pravkar defninirani polinomi so algebarična struktura. Če želimo s polinomi tudi "računati", potrebujemo naslednjo definicijo.

Definicija 1.3. *Naj bo* $P \in A[X]$. *Funkcija* $\widetilde{P} : A \to A$ *je definirana kot*

$$\widetilde{P}(\alpha) = a_0 + a_1\,\alpha + \cdots + a_n\,\alpha^n$$

in ji rečemo polinomska funkcija polinoma P. *Včasih jo označimo kar s* P.

Opomba. *Premislite, ali imata lahko dva različna polinoma iz* $A[X]$ *enako polinomsko funkcijo?*

1.2 Evklidov algoritem

V tem sestavku si bomo na kratko ogledali deljivost polinomov iz $A[X]$ in način, kako polinome delimo.

Definicija 1.4. *Naj bosta* $P_1, P_2 \in A[X]$. *Pravimo, da polinom* P_1 *deli polinom* P_2, *če obstaja polinom* Q, *da velja* $P_2 = P_1 \cdot Q$.

V nadaljevanju si bomo ogledali način, kako ugotovimo, ali nek polinom deli drugega. Dokažimo najprej naslednji izrek.

Izrek 1.1. *Naj bosta* $P_1, P_2 \in A[X]$ *polinoma. Če je* P_2 *monični polinom, potem obstajata taka enolično določena polinoma* $Q, R \in A[X]$, *da je*

$$P_1 = Q\,P_2 + R, \quad \deg(R) < \deg(P_2)\,.$$

Opomba. *Polinom* R *je lahko* 0, *saj je po dogovoru* $\deg(0) = -\infty$, *torej je* $\deg(0) < \deg(P_2)$.

Dokaz. Naj bo $m = \deg(P_1)$ in $n = \deg(P_2)$. Če je $m < n$, vzamemo $Q = 0$ in $R = P_1$.
Naj bo torej $m \geq n$ in $P_1 = a_0 + a_1\,X + \cdots + a_m\,X^m$. Obstoj polinomov Q in R bomo dokazali z indukcijo na m.
Če je $m = n$, je $P_1 = a_m\,P_2 + (P_1 - a_m\,P_2)$ in je $Q = a_m$, $R = P_1 - a_m\,P_2$.

Ker je $\deg(R) < \deg(P_1) = \deg(P_2)$, je obstoj iskanih polinomov Q in R v tem primeru dokazan. Denimo, da je res tudi $P_1 = \widetilde{a}_m P_2 + R_1$, kjer je $\deg(R_1) < \deg(P_2)$. Potem je

$$(a_m - \widetilde{a}_m) P_2 = R - R_1.$$

Toda $\deg(R - R_1) < \deg(P_2)$, polinom P_2 pa je moničen, zato mora biti $(a_m - \widetilde{a}_m) \cdot 1 = 0$. Ker je A brez deliteljev niča, je $a_m = \widetilde{a}_m$. Od tod pa takoj sledi tudi $Q = Q_1$. Torej sta Q in R enolično določena.
Naj bo sedaj $m > n$ in naj izrek drži za naravna števila $n, n+1, \ldots, m-1$. Definirajmo

$$F_1 = P_1 - a_m X^{m-n} P_2.$$

Ker je $\deg(F_1) < \deg(P_1) = m$, po indukcijski predpostavki obstajata enolično določena polinoma Q_1 in R_1, $\deg(R_1) < \deg(P_2)$, da je

$$F_1 = Q_1 P_2 + R_1.$$

Če sedaj za vzamemo $Q = a_m X^{m-n} + Q_1$ in $R = R_1$, je

$$P_1 = Q P_2 + R, \quad \deg(R) < \deg(P_2)$$

in izrek je dokazan. □

Definicija 1.5. *Polinomu R iz prejšnjega izreka rečemo ostanek pri deljenju P_1 s P_2, polinomu Q pa kvocient.*

Opomba. *Zahtevo o moničnosti polinoma P_2 lahko izpustimo, če je A polje ali pa v primeru, ko je vodilni koeficient polinoma P_2 obrnljiv element kolobarja A.*

Deljenje polinoma P_1 s polinomom P_2 je mogoče izvesti algoritmično, torej v končnem številu korakov priti do polinomov Q in R. Postopek je znan kot Evklidov algoritem.

Primer 1.2. *Naj bo $P_1 = 1 + X - X^3 + 2X^4$ in $P_2 = 2 - X + X^2$. Z Evklidovim algoritmom določite kvocient in ostanek pri deljenju polinoma P_1 s P_2.*
Uporabimo algoritem 1.1 in dobimo $Q = -3 + X + 2X^2$ in $R = 7 - 4X$.

Oglejmo si pomembno uporabo Evklidovega algoritma.

Definicija 1.6. *Naj bosta $P_1, P_2 \in A[X]$ polinoma. Polinom $G \in A[X]$ je največji skupni delitelj polinomov P_1 in P_2, če G deli P_1 in P_2 ter za vsak drug delitelj H polinomov P_1 in P_2 velja, da H deli G. Polinom G (če obstaja), bomo označevali z $\gcd(P_1, P_2)$.*

function EVKLID(P_1,P_2)
//Podatki: P_1 in P_2 polinoma, P_2 moničen.
//Rezultat: kvocient Q in ostanek R.
  $R \leftarrow P_1$
  $Q \leftarrow 0$;
  while $\deg(R) \geq \deg(P_2)$ **do**
    $G \leftarrow \mathrm{lc}(R)\, X^{\deg(R)-\deg(P_2)}$
    $Q \leftarrow Q + G$
    $R \leftarrow R - G\, P_2$
  end while
end function

Algoritem 1.1: Evklidov algoritem.

Celostni domeni A, v kateri poljubna dva elementa premoreta največji skupni delitelj, pravimo GCD-domena. Primer take domene je denimo kolobar celih števil. Posebej je vsako polje k (komutativen obseg) GCD-domena. V tem primeru lahko največji skupni delitelj dveh polinomov $P_1, P_2 \in k[X]$ poiščemo z algoritmom 1.2.

PRIMER 1.3. *Z algoritmom 1.2 poiščite največji skupni delitelj polinomov $P_1, P_2 \in \mathbb{Q}[X]$, kjer je*

$$\begin{aligned} P_1(X) &= 1 + 2\,X + 2\,X^2 + X^3 - X^4 - X^5 + X^7 + X^8, \\ P_2(X) &= 2 + X + X^2 + X^4 + X^5. \end{aligned}$$

Dobimo zaporedje $P_1 = Q_1\,P_2 + P_3$, $P_2 = Q_2\,P_3 + P_4$ in $P_3 = Q_3\,P_4 + P_5$, kjer je

$$\begin{aligned} P_3(X) &= 5 + 4\,X + 4\,X^2 - X^3, \\ P_4(X) &= -112(1 + X + X^2), \\ P_5(X) &= 0. \end{aligned}$$

Torej je $\gcd(P_1, P_2) = -112(1 + X + X^2)$.

1.3 Ničle polinomov

V tem razdelku si bomo ogledali nekaj splošnih lastnosti, povezanih z ničlami polinomov. Dogovorimo se najprej, kaj izraz ničla sploh pomeni.

DEFINICIJA 1.7. *Elementu $a \in A$ rečemo ničla polinoma $P \in A[X]$, če je $P(a) = 0$.*

```
function GCD(P1,P2)
//Podatki: P1 in P2 polinoma nad poljem k.
//Rezultat: G ← gcd(P1, P2).
    if P2 = 0 then
        G ← P1
    else
        while P2 ≠ 0 do
            P1 = Q P2 + R //Q in R iz Evklidovega algoritma.
            P1 ← P2
            P2 ← R
        end while
        G ← P1
    end if
end function
```

Algoritem 1.2: Največji skupni delitelj (GCD).

Deljivost in ničlo polinoma povezuje naslednja trditev.

Trditev 1.1. *Naj bo $P \in A[X]$ in $a \in A$. Potem je a ničla polinoma P natanko tedaj, ko polinom $X - a$ deli $P(X)$.*

Dokaz. Po Evklidovem algoritmu obstajata enolično določena polinom $Q \in A[X]$ in element $r \in A$, da je $P(X) = (X - a)\,Q(X) + r$. Če je a ničla P, je $P(a) = r = 0$, torej $(X - a)$ deli $P(X)$. Obratno, če $(X - a)$ deli $P(X)$, je po definiciji $P(X) = Q(X)(X - a)$. Toda potem je $P(a) = 0$ in trditev je dokazana. □

Posledica 1.1. *Če so $a_1, a_2, \ldots, a_m \in A$ različne ničle polinoma $P \in A[X]\backslash 0$, potem polinom $(X - a_1)(X - a_2) \cdots (X - a_m)$ deli $P(X)$ v $A[X]$. Število ničel polinoma P v A je največ* $\deg(P)$.

Dokaz. Dokazovali bomo z indukcijo na m. Za $m = 1$ rezultat sledi iz trditve 1.1. Predpostavimo torej, da izjava iz posledice drži za nek $m \geq 1$. Potem lahko polinom $P(X)$ zapišemo kot

$$P(X) = (X - a_1)(X - a_2) \cdots (X - a_{m-1})Q(X), \quad Q \in A[X]. \tag{1.1}$$

Torej je $P(a_m) = (a_m - a_1)(a_m - a_2) \cdots (a_m - a_{m-1})Q(a_m) = 0$. Ker je A brez deliteljev niča in je $a_m \neq a_i$, $i = 1, 2, \ldots, m - 1$, mora biti $Q(a_m) = 0$. Tedaj pa lahko (ponovno po trditvi 1.1) polinom $Q(X)$ zapišemo kot $Q(X) = (X - a_m)R(X)$, $R \in A[X]$ in iz (1.1) sledi, da $(X - a_1)(X - a_2) \cdots (X - a_m)$

deli $P(X)$ v $A[X]$.
Iz zveze
$$P(X) = (X - a_1)(X - a_2) \cdots (X - a_m)R(X)$$
sledi tudi $m \leq \deg((X - a_1)(X - a_2) \cdots (X - a_m)R(X)) = \deg(P)$, kar je bilo treba dokazati. □

Opomba. *Če ima A delitelje niča, potem obstaja polinom $P \in A[X]$, ki ima več kot* $\deg(P)$ *različnih ničel. Oglejte si denimo polinom $P(X) = a\,X$, kjer je a kak delitelj niča.*

Za polinom $P(X) = 1 - 2\,X + X^2$ iz $\mathbb{Z}[X]$ opazimo, da se da zapisati kot $P(X) = (1 - X)(1 - X) = (1 - X)^2$. Torej ima ničlo $a_1 = 1$, ki se pojavi dvakrat. Taki ničli rečemo večkratna in jo formalno definiramo takole.

Definicija 1.8. *Naj bo $P \in A[X]$ in $a \in A$. Element a je ničla stopnje $k \geq 1$ polinoma $P(X)$, če $(X - a)^k$ deli $P(X)$ v $A[X]$, $(X - a)^{k+1}$ pa ne deli $P(X)$ v $A[X]$. Število k se imenuje večkratnost ničle a.*

Trditev 1.2. *Naj bo $P \in A[X]$ in $a \in A$. Potem je a ničla stopnje $k \geq 1$ natanko tedaj, ko obstaja tak polinom $Q \in A[X]$, da je*
$$P(X) = (X - a)^k Q(X), \quad Q(a) \neq 0.$$

Dokaz. Naj bo a ničla stopnje k. Po definiciji je $P(X) = (X - a)^k Q(X)$. Če bi bilo $Q(a) = 0$, bi po trditvi 1.1 lahko pisali $P(X) = (X - a)^{k+1} Q_1(X)$, kar je v protislovju z definicijo večkratnosti.
Privzemimo sedaj, da je $P(X) = (X - a)^k Q(X)$ in $Q(a) \neq 0$. Denimo, da je tudi $P(X) = (X - a)^{k+1} Q_1(X)$. Potem je $(X - a)^k (Q(X) - (X - a)Q_1(X)) \equiv 0$. Toda $A \neq \{0\}$ je celostno območje, torej je tak tudi kolobar $A[X]$ (poskusite dokazati), zato mora biti $Q(X) = (X - a)Q_1(X)$ in posledično $Q(a) = 0$, kar je protislovje. □

Trditev 1.3. *Če je $P \in A[X] \backslash \{0\}$, potem je vsota večkratnosti ničel polinoma P, ki so v A, največ* $\deg(P)$.

Dokaz. Naj bodo a_i, $i = 1, 2, \ldots, m$, različne ničle polinoma P v A z večkratnostmi s_i, $i = 1, 2, \ldots, m$. Po prejšnji trditvi obstaja tak polinom $Q \in A[X]$, da je
$$P(X) = \prod_{i=1}^{m} (X - a_i)^{s_i} Q(X).$$

Od tod sledi, da je

$$\deg(P) = \deg\left(\prod_{i=1}^{m}(\cdot - a_i)^{s_i}Q\right) \geq \deg\left(\prod_{i=1}^{m}(\cdot - a_i)^{s_i}\right) = \sum_{i=1}^{m} s_i.$$

□

Posledica 1.2. *Naj bo $P \in A[X]$ in $a_i \in A$, $i = 1, 2, \ldots s$, da je $P(a_i) = 0$, $i = 1, 2, \ldots, s$. Če je $s > \deg(P)$, potem je $P = 0$.*

Zadnje trditve omejujejo število ničel polinoma P in karakterizirajo njihovo večkratnost. Ničesar pa ne povedo o eksistenci ničel. V naslednjem poglavju si bomo ogledali poseben primer polinomov, kompleksne polinome, za katere o eksistenci ničel lahko povemo bistveno več.

Poglavje 2

Kompleksni polinomi

V tem poglavju se bomo omejili na poseben primer polinomov, na kompleksne polinome. To so polinomi nad kolobarjem kompleksnih števil, torej $\mathbb{C}[X]$. Pogosto oznako $\mathbb{C}[X]$ zamenjamo z $\mathbb{C}[z]$, kjer z namiguje na spremenljivko, ki jo v polinomski funkciji zamenjamo s kompleksnim številom $z \in \mathbb{C}$. To oznako od sedaj naprej sprejmimo tudi mi.
Izkazalo se bo, da za kompleksne polinome v splošnem lahko povemo nekaj več kot za polinome nad poljubnim celostnim območjem ali poljem.

2.1 Osnovni izrek algebre

Najprej se posvetimo enemu najpomembnejših izrekov algebre, osnovnemu izreku algebre. Že samo ime nakazuje na njegovo pomembnost. Z znanjem, ki smo si ga pridobili v prejšnjem poglavju, osnovni izrek algebre zlahka formuliramo.

Izrek 2.1 (Osnovni izrek algebre). *Vsak nekonstanten polinom $P \in \mathbb{C}[z]$ ima vsaj eno (kompleksno) ničlo.*

Izrek bomo dokazali postopoma, večinoma sledili [3]. Še prej pa podajmo nekaj komentarjev.
Očitno je, zakaj moramo izločiti konstantne polinome. Če je $P(z) = c \in \mathbb{C}\backslash\{0\}$, potem seveda P ne more imeti ničle. Ničelni polinom $P = 0$ pa ima za ničle kar vsa kompleksna števila, kar je druga skrajnost. Prav tako hitro uvidimo, da izrek ne velja za polinome nad poljem realnih števil $\mathbb{R}[x]$. Preprost protiprimer je denimo polinom $P(x) = 1+x^2$, katerega edini ničli sta $\pm i$, ki pa nista v $\mathbb{R}$. Če za vsak nekonstanen polinom $P \in \mathbb{F}[X]$ velja, da ima vse ničle v $\mathbb{F}$, pravimo, da je polje $\mathbb{F}$ algebraično zaprto. Iz osnovnega izreka algebre v resnici sledi, da je polje kompleksnih števil algebraično zaprto.

Preprosto pa je tudi videti, da nobeno končno polje ne more biti algebraično zaprto.

PRIMER 2.1. *Naj bo $\mathbb{F}$ končno polje, katerega elementi so $\{a_0, a_1, \ldots, a_k\}$. Polinom $P(X) = (X - a_0)(X - a_1) \cdots (X - a_k) + 1$ očitno nima ničle v $\mathbb{F}$, torej polje $\mathbb{F}$ ni algebraično zaprto.*

Na poto do dokaza osnovnega izreka algebre bomo najprej dokazali naslednjo pomembno lemo.

LEMA 2.1. *Naj bo $k \in \mathbb{N}$, $k \geq 2$, in $\xi = \left(1 + \frac{i}{k}\right)^2$. Potem je*

$$\operatorname{Re}\left(\xi^k\right) < 0 < \operatorname{Im}\left(\xi^k\right).$$

DOKAZ. Lemo bomo dokazali analitično, le z uporabo polarnega zapisa in prijemi elementarne enalize. Zapišimo ξ v polarni obliki, torej

$$\xi = \left(1 + \frac{1}{k^2}\right)(\cos(2\,\varphi_k) + i\,\sin(2\,\varphi_k)), \quad \varphi_k = \arctan\left(\frac{1}{k}\right).$$

Torej je

$$\xi^k = \left(1 + \frac{1}{k^2}\right)^k (\cos(2\,k\,\varphi_k) + i\,\sin(2\,k\,\varphi_k)).$$

Dovolj je pokazati, da je $2\,k\,\varphi_k \in J := \left(\frac{\pi}{2}, \pi\right)$.
V ta namen si oglejmo funkcijo

$$f(x) = 2\,x\,\arctan\left(\frac{1}{x}\right), \quad x \in I := \left[\sqrt{3}, \infty\right).$$

Lema bo dokazana, če pokažemo, da je $f(I) \subseteq J$.
Ker je

$$f(\sqrt{3}) = 2\sqrt{3}\arctan\left(1/\sqrt{3}\right) = \frac{\sqrt{3}}{3}\pi > \sqrt{3},$$

je $f(\sqrt{3}) \in J$. Zaradi

$$\lim_{x\to\infty} f(x) = \lim_{x\to\infty} 2\frac{\arctan\left(\frac{1}{x}\right)}{\frac{1}{x}} = \lim_{x\to 0} 2\,\frac{\arctan x}{x} = \lim_{x\to 0} 2\,\frac{\frac{1}{1+x^2}}{1} = 2 \in J$$

zadošča preveriti, da je f naraščajoča na I. S preprostim računom pridemo do

$$f'(x) = 2\left(\arctan\left(\frac{1}{x}\right) - \frac{x}{1+x^2}\right).$$

Torej je sedaj dovolj videti, da je $f' > 0$ na I. To pa sledi iz zvez

$$f''(x) = -\frac{4}{(1+x^2)^2}, \quad f'(\sqrt{3}) = \frac{2\,\pi}{6} - \frac{2\,\sqrt{3}}{4} > 0, \quad \lim_{x\to\infty} f'(x) = 0.$$

□

Dokažimo sedaj omenjeni izrek.
Dokaz. Naj bo nekonstanten polinom P oblike $P(z) = a_0 + a_1\,z + \cdots + a_n\,z^n$, kjer so koeficienti $a_j \in \mathbb{C}$, $j = 0, 1, \ldots n$, $a_n \neq 0$, $n \geq 1$. Potem je za vsako kompleksno število $z \in \mathbb{C}$,

$$|P(z)| \geq |a_n|\;|z|^n - |a_{n-1}|\;|z|^{n-1} - \cdots - |a_0|\,.$$

Torej je

$$\lim_{|z|\to\infty} |P(z)| = \infty,$$

od koder sedi, da obstaja tak $R > 0$, da je za vsak $z \in \mathbb{C}$, $|z| > R$, $|P(z)| > |P(w)|$, za vsak $w \in \mathbb{C}$, $|w| \leq R$. Množica $\mathcal{K} := \{w \in \mathbb{C};\ |w| \leq R\}$ je kompaktna, P pa zvezna funkcija, zato $|P|$ zavzame globalni minimum na $\mathcal{K}$. Brez škode za splošnost lahko predpostavimo, da je minimum zavzet pri $z_0 = 0$ (saj sicer na začetku premaknemo koordinatni sistem, da je temu tako). Torej je

$$|P(z)|^2 - |P(0)|^2 \geq 0, \quad \text{za vsak } z \in \mathbb{C}, \tag{2.1}$$

in

$$P(z) = P(0) + z^k\,Q(z), \tag{2.2}$$

za nek $k \in \{1, 2, \ldots, n\}$, kjer je Q polinom, za katerega je $Q(0) \neq 0$. Izberimo poljubno realno število $r \geq 0$ ter poljubno kompleksno število $\zeta \in \mathbb{C}$ in si oglejmo (2.1) pri $z = r\,\zeta$. Po (2.2) je

$$\begin{aligned} |P(z)|^2 &= \overline{(P(0) + z^k\,Q(z))}\,\big(P(0) + z^k\,Q(z)\big) \\ &= |P(0)|^2 + 2\,\mathrm{Re}\left(\left(\overline{P(0)}\,z^k\,Q(z)\right)\right) + \left|z^k\,Q(z)\right|^2, \end{aligned}$$

zato

$$|P(r\,\zeta)|^2 - |P(0)|^2 = 2\,r^k \mathrm{Re}\left(\overline{P(0)}\,\zeta^k\,Q(r\,\zeta)\right) + r^{2\,k}\left|\zeta^k\,Q(r\,\zeta)\right|^2 \geq 0, \quad r \geq 0,$$

oziroma

$$2\,\mathrm{Re}\left(\overline{P(0)}\,\zeta^k\,Q(r\,\zeta)\right) + r^k\left|\zeta^k\,Q(r\,\zeta)\right|^2 \geq 0, \quad r > 0,\ \zeta \in \mathbb{C}.$$

Leva stran zadnje neenačbe je zvezna funkcija r na $[0,\infty)$, zato je po limitiranju $r \to 0$

$$\mathrm{Re}\left(\overline{P(0)}\,Q(0)\zeta^k\right) \geq 0, \quad \text{za vsak } \zeta \in \mathbb{C}. \tag{2.3}$$

Naj bo $\alpha := \overline{P(0)}\,Q(0) = a + i\,b$, $a, b \in \mathbb{R}$. Če je k liho število, potem v (2.3) izberemo za $\zeta = \pm 1$ ter $\zeta = \pm i$ in sklepamo, da je $a = b = 0$. Torej je $\alpha = 0$ in zato $P(0) = 0$, kar pomeni, da ima P vsaj eno ničlo.
Naj bo k sodo število. Če v (2.3) izberemo $\zeta = 1$, sledi $a \geq 0$. Izberimo sedaj ζ tako kot v lemi 2.1 in pišimo $\zeta^k = x + i\,y$. Po pravkar omenjeni lemi je $x < 0$ in $y > 0$. Ker (2.3) velja za ζ in $\overline{\zeta}$, je $\mathrm{Re}\,(\alpha(x \pm i\,y)) = a\,x \mp b\,y \geq 0$. Torej je $a\,x \geq 0$ in zato (ker je $x < 0$) $a \leq 0$. Torej je $a = 0$ in $\mp b\,y \geq 0$. Od tod zaradi $y > 0$ sledi $b = 0$, torej tudi $\alpha = 0$ in $P(0) = 0$. Polinom P ima tudi v tem primeru vsaj eno ničlo. □

Posledica 2.1. *Vsak kompleksni polinom $P \in \mathbb{C}[z]$ stopnje $n \geq 1$ ima natanko n kompleksnih ničel (šteto z večkratnostjo).*

Dokaz. Posledico bomo dokazali z indukcijo na stopnjo n.
Naj bo najprej $n = 1$. Ker polinom stopnje $n = 1$ ne more biti konstanten, ima po prejšnjem izreku vsaj eno ničlo $z_1 \in \mathbb{C}$. Potem je $P(z) = (z - z_1)\,Q(z)$, kjer je Q neničelni konstantni polinom.
Privzemimo sedaj, da ima vsak polinom Q stopnje $n \geq 1$, natanko n kompleksnih ničel. Vzemimo poljuben polinom P stopnje $n+1$. Ponovno ima P po že prej omenjenem izreku vsaj eno kompleksno ničlo z_{n+1}. Zato je

$$P(z) = (z - z_{n+1})\,Q(z), \quad \deg(Q) = n.$$

(Če bi bilo $\deg(Q) < n$, potem P ne bi bil stopnje $n+1$.) Po indukcijski predpostavki ima Q natanko n kompleksnih ničel, ki so seveda tudi ničle polinoma P. Torej ima P natanko $n+1$ kompleksnih ničel, kar smo želeli dokazati. □

Pravkar dokazani izrek očitno ni konstruktiven. Zagotovljen je obstoj n ničel kompleksnega polinoma stopnje n, ni pa jasno, kako jih dobimo. V splošnem lahko ničle kompleksnega polinoma poiščemo le numerično, pa še to ponavadi za polinome, katerih koeficienti so realna števila. Le za polinome stopnje ≤ 4 so znane formule v zaključeni obliki, ki podajajo ničle polinoma kot (eksplicitno) funkcijo koeficientov. Za linearni polinom je to očitno, formule za kvadratni polinom se naučimo v srednji šoli, obstajajo pa še Cardanove formule za kubične polinome in formule za ničle polinoma stopnje 4. Za polinome stopnje ≥ 5 je Niels H. Abel dokazal, da v splošnem

ni mogoče izraziti njihovih ničel z eksplicitnimi algebraičnimi operacijami koeficientov. Obstaja pa nekaj ocen o lokaciji ničel kompleksnega polinoma. Najprej si oglejmo peščico rezultatov, ki locirajo ničle polinoma z realnimi koeficienti (realnega polinoma).

2.2 Descartesovo pravilo predznakov

V tem razdelku si bomo ogledali enega od pomembnejših izrekov o številu pozitivnih realnih ničel realnega polinoma. Izrek je znan pod imenom "Descartesovo pravilo predznakov". Še prej si oglejmo nekaj splošnih rezultatov o število pozitivnih in negativnih ničel realnega polinoma. Kot smo navajeni, pišimo nedoločenko kot x, polinom $p \in \mathbb{R}[x]$ pa kot

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

Iz koeficientov polinoma p, lahko tvorimo zaporedje $n+1$ realnih števil, ki ga označimo kot vektor

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_n). \tag{2.4}$$

V nadaljevanju bomo potrebovali naslednjo definicijo.

Definicija 2.1. *Pravimo, da sta neničelna člena a_i in a_j zaporedja* (2.4) *zaporedna, če je $j = i+1$, ali pa je $j > i+1$ in je $a_k = 0$ za $k = i+1, i+2, \ldots, j-1$. Sprememba predznaka v zaporedju je par zaporednih členov zaporedja z različnim predznakom. Število sprememb predznaka označimo z $V(\boldsymbol{a}) := V(a_0, a_1, \ldots, a_n)$.*

Primer 2.2. *V zaporedju* -2, 3, 4, -1, -2, 2, 3 *so tri spremembe predznaka, zato je $V(-2, 3, 4, -1, -2, 2, 3) = 3$. V zaporedju* 3, 0, 0, -1, 1, 3, 0 *pa sta dve spremembi predznaka (par* 3, -1 *in par* -1, 1*), zato je $V(3, 0, 0, -1, 1, 3, 0) = 2$.*

Najprej dokažimo nekaj preprostejših rezultatov.

Lema 2.2. *Če so vsi koeficienti polinoma p pozitivni, potem p nima pozitivnih realnih ničel.*

Dokaz. Če so vsi koeficienti a_i, $i = 0, 1, \ldots, n$, pozitivni, je za vsak $x > 0$ vrednost $p(x)$ očitno pozitivna, torej p nima ničel na $(0, \infty)$. □

Posledica 2.2. *Če je za polinom p število sprememb predznaka $V(\boldsymbol{a}) = n$, potem p nima negativnih ničel.*

Dokaz zadnje posledice prepuščamo bralcu, oglejmo pa si primer uporabe zadnjih dveh trditev.

PRIMER 2.3. *Polinom* $p(x) = x^4 + 10\,x^3 + 35\,x^2 + 50\,x + 24$ *po lemi 2.2 nima pozitivnih ničel. Bralec se res lahko prepriča, da ima ničle pri* $x = -1, -2, -3, -4$.
Po posledici 2.2 pa polinom $p(x) = x^4 - 10\,x^3 + 35\,x^2 - 50\,x + 24$ *nima negativnih ničel. Njegove ničle so* $x = 1, 2, 3, 4$.

TRDITEV 2.1. *Če so vse ničle polinoma* p *stopnje* $n \geq 1$ *pozitivne, potem je* $V(\boldsymbol{a}) = n$.

DOKAZ. Dokazujmo z indukcijo na n. Za $n = 1$ dejstvo, da ima $p(x) = a_1\,x + a_0$ pozitivno ničlo pomeni, da je $a_1\,a_0 < 0$, torej je $V(\boldsymbol{a}) = 1$. Naj bo sedaj $p(x) = a_{n+1}\,x^{n+1} + a_n\,x^n + \cdots + a_1\,x + a_0$ polinom stopnje $n+1$ s samimi pozitivnimi ničlami ξ_i, $i = 1, 2, \ldots, n+1$. Potem je

$$p(x) = a_{n+1}(x - \xi_1)(x - \xi_2)\cdots(x - \xi_{n+1}).$$

Torej je

$$p(x) = (x - \xi_{n+1})q(x), \tag{2.5}$$

kjer je

$$q(x) = a_{n+1}\,(x - \xi_1)(x - \xi_2)\cdots(x - \xi_n) = b_n\,x^n + b_{n-1}\,x^{n-1} + \cdots + b_1\,x + b_0. \tag{2.6}$$

Polinom q ima same pozitivne ničle, zato je po indukcijski predpostavki $V(\boldsymbol{b}) = n$. Iz zvez (2.5) in (2.6) sledi

$$\begin{aligned} a_0 &= -\xi_{n+1}\,b_0, \\ a_i &= b_{i-1} - \xi_{n+1}\,b_i, \quad i = 1, 2, \ldots, n, \\ a_{n+1} &= b_n, \end{aligned}$$

od tod pa zlahka preverimo, da je $V(\boldsymbol{a}) = n+1$ (saj opazimo, da je predznak b_n enak predznaku a_{n+1}, predznak b_{n-1} enak predznaku a_n,..., predznak b_0 enak predznaku a_1 in zato predznak a_0 nasproten predznaku a_1). □

POSLEDICA 2.3. *Če so vse ničle polinoma* p *stopnje* n *negativne, potem je* $V(\boldsymbol{a}) = 0$.

Tudi dokaz te posledice prepuščamo bralcu.

Obrat pravkar zapisane trditve (in posledice) ne velja.

PRIMER 2.4. *Polinom* $p(x) = (x - 1/3)(x - 1/2)(x - 2)(x - 3)$ *ima same pozitivne ničle. Ko ga razpišemo po potencah, dobimo*

$$p(x) = x^4 - \frac{35}{6}x^3 + \frac{31}{3}x^2 - \frac{35}{6}x + 1,$$

torej ima vse koeficinete neničelne z alternirajočimi predznaki.
Po drugi strani pa polinom $p(x) = x^2 + x + 1$ *nima nobene realne ničle (kaj šele vse negativne), pa čeprav so vsi koeficienti neničelni in istega predznaka. To dokazuje, da obrat posledice 2.3 ni mogoč. Podobno dobimo protiprimer tudi za trditev 2.1.*

Sedaj bomo dokazali prvi korak k omenjenemu Descartesovemu izreku. Pokazali bomo, da natanko ena sprememba predznaka v koeficientih polinoma p implicira obstoj natanko ene pozitivne ničle polinoma. Še prej dokažimo naslednji izrek.

IZREK 2.2. *Če je v polinomu* p *stopnje* n *s pozitivnim vodilnim koeficientom pred prvim negativnim koeficientom (gledano od vodilnega koeficienta proti prostemu členu) natanko* k *pozitivnih ali ničelnih koeficientov in* N *označuje absolutno vrednost največjega negativnega koeficienta, potem je* $p(x) > 0$ *za* $x \geq 1 + \sqrt[k]{N/a_n}$. *Polinom* p *ima tedaj torej vse realne ničle na intervalu* $(-\infty, 1 + \sqrt[k]{N/a_n})$.

DOKAZ. Naj za koeficiente a_i, $i = 0, 1, \ldots, n$, v polinomu $p(x) = a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_{n-k+1}\, x^{n-k+1} + a_{n-k}\, x^{n-k} + \cdots + a_1\, x + a_0$ velja $a_n > 0$, $a_i \geq 0$, $i = n-k+1, n-k+2, \ldots, n-1$ in $a_{n-k} < 0$. Potem je za $x > 1$

$$p(x) \geq a_n\, x^n + \sum_{j=0}^{n-k} a_j\, x^j \geq a_n\, x^n - \sum_{j=0}^{n-k} N\, x^j,$$

kjer je

$$N = \max\left\{|a_j|;\ \operatorname{sign}(a_j) = -1,\ 0 \leq j \leq n-k\right\}.$$

Od tod dobimo

$$p(x) > a_n\, x^{k-1}\left(x^{n-k+1} - 1\right) - N\frac{x^{n-k+1} - 1}{x - 1} > \frac{x^{n-k+1} - 1}{x - 1}\left(a_n(x-1)^k - N\right).$$

Ker je $x > 1$, je prvi faktor na desni strani zadnje neenakosti pozitiven. Če je $x \geq 1 + \sqrt[k]{N/a_n}$, je nenegativen še drugi faktor in izrek je dokazan. □

TRDITEV 2.2. *Če za polinom* p *velja* $V(\boldsymbol{a}) = 1$, *potem ima* p *vsaj eno pozitivno ničlo.*

Dokaz. Brez škode za splošnost lahko predpostavimo, da je $a_0 \neq 0$ (sicer izločimo (večkratno) ničlo $x = 0$). Tedaj iz predpostavke trditve sledi, da je $a_n\, a_0 < 0$. Torej je bodisi $p(0) < 0$ in $p(x) > 0$ za dovolj velike x, bodisi $p(0) > 0$ in $p(x) < 0$ za dovolj velike x. Zaradi zveznosti funkcije p ima slednja vsaj eno ničlo na $(0, \infty)$. □

Za dokaz obstoja natanko ene pozitivne ničle bomo uporabili nekaj lastnosti funkcije $\phi_k(x) = \sum_{j=0}^{k-1} x^j$, $k = 1, 2, \ldots$ Te so:

$$\phi_k(1) = k, \tag{2.7}$$

$$\phi_k(y) \geq \phi_k(x), \quad y \geq x \geq 1, \tag{2.8}$$

$$\phi_\ell(x) \geq \phi_k(x), \quad \ell \geq k, \quad x \geq 0. \tag{2.9}$$

Trditev 2.3. *Če za polinom p velja $V(\boldsymbol{a}) = 1$, potem ima p* **natanko eno** *pozitivno ničlo.*

Dokaz. Brez škode za splošnost lahko privzememo, da je vodilni koeficient polinoma p pozitiven in prosti člen različen od 0 (sicer polinom pomnožimo z -1 in izločimo morebitno večkratno ničlo pri 0, kar ne spremeni vrednosti $V(\boldsymbol{a})$). Po prejšnji trditvi obstaja vsaj ena pozitivna ničla polinoma p. Dokazati moramo, da je edina. Privzemimo, da je pozitivnih ničel več in z α označimo najmanjšo med njimi. Definirajmo polinom $\hat{p}(x) = \alpha^{-n}\, p(\alpha\, x)$. Koeficienti polinoma $\hat{p}$ imajo enake predznake kot koeficienti polinoma p. Najmanjša ničla polinoma $\hat{p}$ pa je $x = 1$. Pokazali bomo, da je $x = 1$ enostavna ničla polinoma $\hat{p}$ in je $\hat{p}(x) > 0$ za $x > 1$.
Ker je $a_n > 0$ po privzetku, lahko $\hat{p}$ zapišemo kot

$$\hat{p}(x) = \sum_{j=n-k+1}^{n} b_j\, x^j - \sum_{j=0}^{n-k} |b_j|\; x^j, \quad 1 \leq k \leq n,$$

kjer je $b_j \geq 0$, $j = n-k+1, \ldots, n$ in $b_j \leq 0$, $j = 0, 1, \ldots, n-k$. Potem je

$$\begin{aligned}\hat{p}(x) = \hat{p}(x) - \hat{p}(1) &= \sum_{j=n-k+1}^{n} b_j (x^j - 1) - \sum_{j=0}^{n-k} |b_j|\, (x^j - 1) \\ &= (x-1) \left(\sum_{j=n-k+1}^{n} b_j\, \phi_j(x) - \sum_{j=1}^{n-k} |b_j|\, \phi_j(x) \right) = (x-1)\, s(x),\end{aligned}$$

kjer je

$$s(x) := \left(\sum_{j=n-k+1}^{n} b_j\, \phi_j(x) - \sum_{j=1}^{n-k} |b_j|\, \phi_j(x) \right).$$

Dovolj je videti, da je s pozitivna funkcija na $[1, \infty)$. Naj bo torej $x \geq 1$. S pomočjo lastnosti (2.7)–(2.9) ocenimo

$$\begin{aligned} s(x) &\geq \phi_{n-k+1}(x) \left(\sum_{j=n-k+1}^{n} b_j - \sum_{j=1}^{n-k} |b_j| \right) \\ &= \phi_{n-k+1}(x) \left(\sum_{j=n-k+1}^{n} b_j - \sum_{j=0}^{n-k} |b_j| + |b_0| \right) \geq \phi_{n-k+1}(1) \left(\hat{p}(1) + b_0 | \right) \\ &= (n-k+1)|b_0| > 0 \end{aligned}$$

in izrek je dokazan. □

Še nekaj splošnih rezultatov o pozitivnih ničlah realnega polinoma bralec lahko najde v [1]. Mi pa se bomo v nadaljevanju posvetili primeru, ko koeficienti realnega polinoma več kot enkrat spremenijo predzak. V tem primeru ne moremo dokazati, da je pozitivnih ničel ravno toliko kot sprememb predznaka.

Primer 2.5. *Polinom $p(x) = x^2 - x + 2$ ima v zaporedju koeficientov 2, -1, 1 dve spremembi predznaka, vendar nima pozitivnih ničel (sploh nima realnih ničel).*

Oglejmo si sedaj nekaj splošnih rezultatov, ki se nanašajo na zaporedje (2.4) in $V(\boldsymbol{a})$. Najprej opazimo naslednje.

Lema 2.3. *Prvi in zadnji neničelni element v zaporedju* (2.4) *imata isti (nasprotni) predznak natanko tedaj, ko je $V(\boldsymbol{a})$ sodo (liho) število.*

Iz prejšnje leme neposredno sledi naslednji rezultat.

Lema 2.4. *Naj bo $r_0, r_1, \ldots, r_{n-1}$ zaporedje pozitivnih števil. Definirajmo zaporedje $V(\boldsymbol{b}) = (b_j)_{j=0}^n$ takole:*

$$\begin{aligned} b_0 &= a_0, \\ b_j &= a_j + r_{j-1}\, b_{j-1}, \quad j = 1, 2, \ldots, n. \end{aligned} \tag{2.10}$$

Če so a_0, a_n in b_n vsi neničelni in je $V(\boldsymbol{a}) = V(\boldsymbol{b})$, sta predznaka števil a_n in b_n enaka.

Dokaz. Ker je $V(\boldsymbol{a}) = V(\boldsymbol{b})$, sta $V(\boldsymbol{a})$ in $V(\boldsymbol{b})$ seveda iste parnosti, zato sta po prejšnji lemi produkta $a_0\, a_n$ in $b_0\, b_n$ istega predznaka. Ker je po definiciji $a_0 = b_0$ in po privzetku $a_0\, a_n\, b_n \neq 0$, morata biti a_n in b_n istega predznaka. □

Tudi naslednji razmislek je prepost in ga prepuščamo bralcu.

LEMA 2.5. *Naj bo* $\boldsymbol{a} = (a_0, a_1, \ldots, a_n)$ *in* $\widetilde{\boldsymbol{a}} = (a_0, a_1, \ldots, a_n, a_{n+1})$. *Potem je* $V(\boldsymbol{a}) \leq V(\widetilde{\boldsymbol{a}}) \leq V(\boldsymbol{a}) + 1$.

Sedaj pa bomo z indukcijo dokazali malce globji rezultat.

LEMA 2.6. *Naj bo zaporedje* $\boldsymbol{b} = (b_0, b_1, \ldots, b_n)$ *definirano z* (2.10) *kot v lemi 2.4. Potem je* $V(\boldsymbol{b}) \leq V(\boldsymbol{a})$. *Če sta števili* $a_0\, a_n \neq 0$ *in* $b_n = 0$, *pa je* $V(\boldsymbol{b}) < V(\boldsymbol{a})$.

DOKAZ. Naj bo $n = 1$. Potem je lahko $V(\boldsymbol{a})$ le 0 ali 1, odvisno od tega ali je produkt $a_0\, a_1$ nenegativen ali negativen. Iz definicije zaporedja $\boldsymbol{b}$ sledi $b_1\, b_0 = a_1\, a_0 + r_0\, a_0^2$. Če je produkt $a_0\, a_1$ nenegativen, je tak tudi produkt $b_1\, b_0$ in število sprememb predznaka je v obeh zaporedjih 0. V primeru, da je $a_0 \neq 0$, je $b_1\, b_0 > 0$ in zato b_1 ne more biti 0. Če je produkt $a_0\, a_1$ negativen, je $V(\boldsymbol{a}) = 1 \geq V(\boldsymbol{b})$ in $V(\boldsymbol{a}) > V(\boldsymbol{b})$ v primeru, ko je $b_1 = 0$.
Predpostavimo sedaj, da lema drži za vse pare zaporedij dolžine $n + 1$, ki zadoščajo predpostavkam. Izberimo dve zaporedji $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n+1})$ in $\boldsymbol{b} = (b_0, b_1, \ldots, b_{n+1})$, kjer so členi zaporedja $\boldsymbol{b}$ definirani z rekurzijo (2.10).
Če je $a_0 = 0$, je tudi $b_0 = 0$, zato imata zaporedji $a_1, a_2, \ldots, a_{n+1}$ in $b_1, b_2, \ldots, b_{n+1}$ enako število sprememb predznaka kot zaporednji $\boldsymbol{a}$ in $\boldsymbol{b}$ ter zadoščata pogojem v lemi. Rezultat leme tedaj sledi iz indukcijske predpostavke.
Če je $a_j = 0$, za nek $j > 0$, potem je $b_j = a_j + r_{j-1}\, b_{j-1}$ istega znaka kot b_{j-1}. Torej lahko iz zaporedja $\boldsymbol{a}$ brišemo a_j, iz zaporedja $\boldsymbol{b}$ pa b_j, ne da bi spremenili število sprememb predznaka v enem ali drugem zaporedju. Še več, novonastalo zaporedje $b_0, b_1, \ldots, b_{j-1}, b_{j+1}, \ldots, b_{n+1}$ je ponovno dobljeno na podlagi rekurzije (2.10), saj je $b_{j+1} = a_{j+1} + r_j\, b_j = a_{j+1} + r_j\, r_{j-1}\, b_{j-1}$. Zato rezultat ponovno sledi iz indukcijske predpostavke.
Oglejmo si še primer, ko so vsa števila a_j, $j = 0, 1, \ldots, n + 1$, neničelna.
Najprej opazimo, da je

$$V(b_0, b_1, \ldots, b_n) \leq V(a_0, a_1, \ldots, a_n) \leq V(a_0, a_1, \ldots, a_n, a_{n+1}).$$

Prva neenakost sledi iz indukcijske predpostavke, druga pa iz leme 2.5. Naj bo $b_{n+1} = 0$. Po indukcijski predpostavki je

$$V(b_0, b_1, \ldots, b_n) \leq V(a_0, a_1, \ldots, a_n).$$

Če je $V(b_0, b_1, \ldots, b_n) < (a_0, a_1, \ldots, a_n)$, je tudi $V(\boldsymbol{b}) < V(\boldsymbol{a})$. Če pa je $V(b_0, b_1, \ldots, b_n) = V(a_0, a_1, \ldots, a_n)$, je po indukcijski predpostavki $b_n \neq 0$ in ima po lemi 2.4 enak predznak kot a_n. Toda potem iz $0 = b_{n+1} = a_{n+1} + r_n\, b_n$ sledi, da imata a_{n+1} in b_n različen predznak, zato je $V(\boldsymbol{b}) < V(\boldsymbol{a}$.
Ostane še primer, ko je $b_{n+1} \neq 0$. Po indukcijski predpostavki je ponovno $V(b_0, b_1, \ldots, b_n) \leq V(a_0, a_1, \ldots, a_n)$. Če je neenakost stroga, je lema dokazana,

saj je tedaj v vsakem primeru $V(\boldsymbol{b}) \leq V(\boldsymbol{a})$. Privzemimo, da je torej $V(b_0, b_1, \ldots, b_n) = V(a_0, a_1, \ldots, a_n)$. Dokazati moramo, da je tudi v tem primeru $V(\boldsymbol{b}) \leq V(\boldsymbol{a})$. Privzemimo nasprotno, torej $V(\boldsymbol{b}) > V(\boldsymbol{a})$. Torej je $b_n\, b_{n+1} < 0$ in $a_n\, a_{n+1} > 0$. Števili a_n in b_n imata enak predznak, ponovno po lemi 2.4. Toda potem je po privzetku

$$b_n\, b_{n+1} = b_n\, a_{n+1} + b_n^2\, r_n < 0,$$

torej tudi $a_{n+1}\, b_n < 0$ in posledično $a_{n+1}\, a_n < 0$, kar je protislovje. Izrek je dokončno dokazan. □

Sedaj bomo pravkar izpeljane rezultate uporabili za določanje števila pozitivnih ničel polinoma $p(x) = a_n\, x^n + \cdots a_1\, x + a_0$. Najprej dokažimo naslednjo lemo.

Lema 2.7. *Naj bo $a_0\, a_n \neq 0$. Potem ima polinom p sodo (liho) število pozitivnih ničel, če je $a_0\, a_n > 0$ ($a_0\, a_n < 0$).*

Dokaz. Opazimo, da ima polinom $q(x) = x^n + c_{n-1}\, x^{n-1} + \cdots + c_1\, x + c_0$, kjer je $c_i = a_i/a_n$, $i = 0, 1, \ldots, n$, iste ničle kot p. Predznak c_0 je isti kot predznak $a_0\, a_n$, saj je $c_0 = (a_0\, a_n)/a_n^2$. Obenem je $q(0) = c_0$ in $q(x) > 0$ za $x > M$, kjer je M neko dovolj veliko število. To pomeni, da vse pozitivne ničle polinoma q ležijo na intervalu $I = (0, M)$. Zlahka se prepičamo, da je na I liho mnogo ničel, če je $c_0 < 0$, in sodo mnogo ničel, če je $c_0 > 0$. □

Sedaj lahko dokažemo glavni izrek tega poglavja.

Izrek 2.3 (Descartesovo pravilo predznakov). *Naj bo $p(x) = a_n\, x^n + a_{n-1}\, x^{n-1} + \cdots + a_1\, x + a_0$ polinom z realnimi koeficienti in τ število pozitivnih ničel polinoma p. Potem je*

$$V(\boldsymbol{a}) - \tau = 2\, k, \quad k \in \mathbb{N}.$$

Dokaz. Brez škode za splošnost lahko predpostavimo, da sta a_0 in a_n neničelna (sicer se stopnja polinoma zmanjša, ali pa izločimo (večkratno) ničlo pri 0). Prav tako hitro vidimo, da je

$$\hat{p}(1/x) = \frac{p(x)}{x^n},$$

kjer je

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

Ker imata p in $\hat{p}$ enako število pozitivnih ničel in je $V(a_0, a_1, \ldots, a_n) = V(a_n, a_{n-1}, \ldots, a_1, a_0)$, lahko izrek dokažemo za $\hat{p}$.

Naj bo ρ pozitivna ničla polinoma $\hat{p}$. Potem je $\hat{p}(x) = (x - \rho)q(x)$, kjer je $q(x) = b_0\, x^{n-1} + b_1\, x^{n-2} + \cdots + b_{n-2}\, x + b_{n-1}$ in se b_i izražajo kot

$$\begin{aligned} b_0 &= 0, \\ b_j &= a_j + \rho\, b_{j-1}, \quad j = 1, 2, \ldots, n-1, \\ b_n &= 0. \end{aligned}$$

Po lemi 2.6 (vzamemo $r_j \equiv \rho$) je $V(\boldsymbol{b}) \leq V(\boldsymbol{a}) - 1$. Po τ korakih dobimo $0 \leq V(\boldsymbol{a}) - \tau$, oziroma $V(\boldsymbol{a}) \geq \tau$. Toda kriterij za sodost ali lihost $V(\boldsymbol{a})$ in τ je po lemah 2.3 in 2.7 isti, zato je nujna razlika sodo število in izrek je dokazan. □

Kaj pa število negativnih ničel polinoma? S preprostim trikom lahko ta problem prevedemo na določanje števila pozitivnih ničel ustreznega polinoma. Opazimo namreč, da je število negativnih ničel polinoma $p(x) = a_n\, x^n + \cdots + a_1\, x + a_0$ enako število pozitivnih ničel polinoma $p(-x) = (-1)^n\, a_n\, x^n + \cdots + (-1)\, a_1 + a_0$. Zanj pa lahko uporabimo Descartesovo pravilo predznakov.

Primer 2.6. *Locirajmo število ničel polinoma* $p(x) = x^4 - 2\, x^3 - x^2 - 6$ *glede na njihov predznak. Število sprememb predznaka v zaporedju* $-6, 0, -1, -2, 1$ *je* 1*, torej ima* p *natanko eno pozitivno ničlo. Polinom* $q(x) = p(-x) = x^4 + 2\, x^3 - x^2 - 6$ *ima v zaporedju koeficientov* $-6, 0, -1, 2, 1$ *eno spremembo predznaka, zato ima* q *natanko eno pozitivno ničlo, torej ima* p *natanko eno negativno ničlo. Zaključimo lahko, da ima* p *natanko eno pozitivno in natanko eno negativno ničlo ter dve konjugirano kompleksni ničli.*

Poglavje 3

Dodatek

V tem poglavju bomo podrobneje definirali nekaj algebrskih struktur, ki jih omenjamo v prejšnjih poglavjih. Začnimo z definicijo notranje binarne operacije.

Definicija 3.1. *Notranja binarna operacija na neprazni množici A je vsaka preslikava $\circ : A \times A \to A$, ki vsakemu paru elementoc $a, b \in A$ priredi natanko določen element $c \in A$. To ponavadi zapišemo takole*

$$a \circ b = c.$$

Množici A, opremljeni z notranjo operacijo, rečemo grupoid.
Element $e \in A$ je v grupoidu leva enota (levi nevtralni element), če je $e \circ x = x$ za vsak $x \in A$. Podobno je e desna enota (desni nevtralni element), če je $x \circ e = x$ za vsak $x \in A$. Če je element hkrati leva in desna enota ga imenujemo enota ali nevtralni element.
V grupoidu z enoto e je element $a' \in A$ je levi inverzni element k $a \in A$, če je $a' \circ a = e$. Podobno je $a' \in A$ desni inverzni element k elementu a, če je $a \circ a' = e$. Če pa za element $a' \in A$ velja, da je $a' \circ a = a \circ a' = e$, je a' inverzni element k elementu a. Elementu a tedaj rečemo, da je obrnljiv element.

Pogosto grupoid označimo kot urejen par $(A, \circ)$,

Definicija 3.2. *Če je v grupoidu $(A, \circ)$ operacija $\circ$ asociativna, torej, če za vsako trojico elementov $a, b, c \in A$ velja*

$$(a \circ b) \circ c = a \circ (b \circ c),$$

potem grupoidu rečemo polgrupa ali monoid.

Primer polgrupe so denimo naravna števila za operacijo seštevanja. Element 0 je enota tega grupoida, noben element pa ni obrnljiv (niti z leve, niti z desne).

Definicija 3.3. *Polgrupo $(A, \circ)$ z enoto, v kateri so vsi elementi obrnljivi, imenujemo grupa. Grupa je Abelova (ali komutativna), če je operacija $\circ$ komutativna, torej, če za vsak par $a, b \in A$ velja $a \circ b = b \circ a$.*

Cela števila $\mathbb{Z}$ za operacijo seštevanja so Abelova grupa. Enota je število 0, elementu $a \in \mathbb{Z}$ inverzni element pa je $-a$.

Definicija 3.4. *Denimo, da imamo v množici A dve notranji operaciji, označimo ju z $+$ (adicija) in $\cdot$ (multiplikacija). Naj bo operacija $\cdot$ distibutivna glede na $+$, to pomeni, da za vsako trojico $x, y, z \in A$ velja*

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z),$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z).$$

Pravimo, da je $(A, +, \cdot)$ kolobar, če je

- *$(A, +)$ Abelova grupa,*
- *$(A, \cdot)$ polgrupa,*
- *multiplikacija distributivna glede na adicijo.*

Če je multiplikacija $\cdot$ komutativna, imenujemo kolobar $(A, +, \cdot)$ komutativen. Če je $(A, \cdot)$ polgrupa z enoto, bomo to enoto označili z 1 in ga imenovali enota kolobarja. V tem primeru bomo rekli, da je $(A, +, \cdot)$ kolobar z enoto.

Primer komutativnega kolobarja z enoto je kolobar $(\mathbb{Z}, +, \cdot)$, kjer sta $+$ in $\cdot$ običajno seštevanje in množenje celih števil.

Definicija 3.5. *Če v kolobarju $(A, +, \cdot)$ za elementa $a, b \neq 0$, kjer je 0 enota v Abelovi grupi $(A, +)$, velja, da je $a \cdot b = 0$, je a levi, b pa desni delitelj niča. Kolobar, ki nima deliteljev niča, se imenuje kolobar brez deliteljev niča.*

Kolobar ostankov pri deljenju s 4 je primer kolobarja, ki ima delitelje niča. Katere?

Definicija 3.6. *Komutativnemu kolobarju z enoto in brez deliteljev niča rečemo celostno polje.*

Definicija 3.7. *Kolobar $(A, +, \cdot)$ z enoto je obseg natanko tedaj, ko so vsi neničelni elementi (torej tisti, ki niso enaki enoti za multiplikativno grupo $(A, +)$) obrnljivi. Obseg je komutativen, če je kolobar komutativen. Takemu obsegu rečemo polje.*

Primer komutativnega obsega so realna števila $\mathbb{R}$ za običajno seštevanje in množenje.

Literatura

[1] A. S. Levin. Descartes' rule of signs–how hard can it be? *Preprint*, 2002.

[2] M. Mignotte and D. Ştefănescu. *Polynomials. An algorithmic approach.* Springer, Singapore, 1999.

[3] O. Oliveira. The fundamental theorem of algebra: An elementary and direct proof. *Math. Intelligencer*, 33:1–2, 2011.

[4] E. Zakrajšek. *Matematično modeliranje.* Matematika - fizika. DMFA - založništvo, 2004.