# Polinomi 0

Ali: "Več o tem kasneje."

Luka Urbanc

Avgust 2023

Najprej se opravičujem za suhoparnost. Žal je iz teh osnov polinomske aritmetike težko najti zanimive naloge/primere – so pač osnove. Zato pa jih je treba dobro poznati, če hočeš pozneje razumeti in dokazovati zanimivejše izjave.

## 1 $\mathbb{F}[x]$

Kaj sploh so polinomi? Preprosto povedano so to objekti oblike $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.[1] Tukaj bodo $a_i$ običajno elementi nekega *polja*.[2]

**Definicija 1.1** (Polje)**.** Polje, ki ga v splošnem označujem s $\mathbb{F}$ (field), je množica z dvema binarnima operacijama (binarne operacije so funkcije $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$): s seštevanjem $(+)$ in z množenjem $(\cdot)$. **Ideja je, da se te operacije obnašajo enako, kot se pri npr. realnih ali racionalnih številih**, zato zahtevamo, da zanje velja nekaj aksiomov:

- (Komutativnost, asociativnost, distributivnost) Za vse $a, b, c \in \mathbb{F}$ velja $a + b = b + a,\ a \cdot b = b \cdot a,\ a + (b + c) = (a + b) + c,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c,\ a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
- (Identitete) Obstajata dva različna elementa 0 in 1, za katera velja $a + 0 = a,\ a \cdot 1 = a$ za vse $a \in \mathbb{F}$ (da se dokazati, da sta identiteti edinstveni).
- (Inverzi) Za vsak $a \in \mathbb{F}$ obstaja element $-a$, da je $a + (-a) = 0$, in za vsak $a \in \mathbb{F},\ a \neq 0$ obstaja element $a^{-1}$, za katerega je $a \cdot a^{-1} = 1$ (prav tako sledi, da za vse $a \in \mathbb{F}$ obstaja natanko en aditivni in, razen za $a = 0$, natanko en multiplikativni inverz).

[1] Obstajajo tudi polinomi z več spremenljivkami; ti so bolj kompliciran. Več o njih morda kasneje.

[2] Če so koeficienti v polju, se množica polinomov obnaša "podobno" kot $\mathbb{Z}$ (!!!). Sicer bi se spodobilo razviti tudi teorijo polinomov s koeficienti v kolobarjih, a je to nekoliko manj intuitivno in se v olimpijski matematiki pojavlja le pri polinomih s koeficienti iz $\mathbb{Z}$. To pa je relativno lahek primer, v grobem zaradi Gaussove leme, ki nam zagotavlja, da je skoraj ekvivalenten primeru $\mathbb{Q}[x]$. Več o njej kasneje.

Primeri polj so $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ in $\mathbb{Z}/p\mathbb{Z}$ z običajnimi operacijami seštevanja in množenja. Zadnji primer je posebej zanimiv, ker je množica končna: takim poljem pravimo (drum roll please...) **končna polja**. Več o njih kasneje.
$\mathbb{Z}$ ni polje, ker nekateri neničelni elementi nimajo multiplikativnih inverzov: $2x = 1$ nima rešitev za $x \in \mathbb{Z}$. Takim objektom pravimo **kolobarji**. Gre preprosto za polja brez multiplikativnih inverzov (pri katerih je dovoljeno $0 = 1$...), kjer množenje ni nujno komutativno, ko pa je, kolobarju pravimo komutativen. ($\mathbb{Z}$ je torej komutativni kolobar).

Najprej: splošni element množice $\mathbb{F}[x]$ je $p(x) = \sum_{k=0}^{m} a_k x^k$. Dva elementa sta enaka, če in samo če so vsi koeficienti enaki v $\mathbb{F}$, torej če označimo

$$p(x) = \sum_{k=0}^{m} a_k x^k,\ q(x) = \sum_{k=0}^{n} b_k x^k,$$

potem velja $p(x) = q(x) \iff a_k = b_k,\ \forall 0 \leq k \leq \max(m, n)$.

Prav tako imamo operaciji seštevanja in množenja, ki sta definirani tako, kot bi človek pričakoval. Obstajata tudi identiteti za seštevanje in množenje ter veljajo komutativnost, asociativnost in distributivnost. Imamo aditivne inverze, na žalost pa v splošnem ni multiplikativnih inverzov. Torej je naša množica komutativni kolobar, tako kot $\mathbb{Z}$.

Vsakemu elementu lahko pripišemo **stopnjo**, ki je največje celo število $d$, za katero $a_d \neq 0$ (stopnja ničelnega polinoma je definirana kot $-\infty$). To je torej funkcija $d : \mathbb{F}[x] \to \mathbb{N}_0 \cup \{-\infty\}$. Njena najpomembnejša lastnost je, da množenje polinomov "pretvori" v seštevanje nenegativnih celih števil (in $-\infty$: definiramo $a + (-\infty) = -\infty$ za vse $a$). Torej $d(p(x) \cdot q(x)) = d(p(x)) + d(q(x))$; lahko bi rekli, da se obnaša zelo podobno logaritemski funkciji absolutne vrednosti v $\mathbb{Z}$. Polinomom stopnje $\leq 0$ pravimo konstantni.

## 2 ÷

Najzanimivejša operacija v $\mathbb{F}[x]$ pa je verjetno deljenje. (Seveda gre tu za deljenje z ostanki, ker večina elementov nima multiplikativnih inverzov.)

**Izrek 2.1** (Deljenje polinomov)**.** *Za vsak par polinomov $a(x), b(x)$, kjer $b(x) \neq 0$, obstaja enolično določen par polinomov $q(x), r(x)$, za katera velja $d(r(x)) < d(b(x))$ in $a(x) = b(x) \cdot q(x) + r(x)$.*

Najti dokaz za ta izrek je dobra vaja. Najboljši način, ki ga poznam, je da spišeš algoritem za deljenje in dokažeš, da deluje (namiga: glej vodilne koeficiente; stopnja je monovarianta). Če to narediš, opaziš še, da skoraj enak dokaz deluje tudi za $\mathbb{Z}$, le da tam vlogo monovariante prevzame absolutna vrednost

(moramo paziti le, da je ostanek vedno pozitiven).

Ostanek pri deljenju $a(x)$ z $b(x)$ bom od tu dalje označeval z $r_{a,b}(x)$, kvocient pa s $q_{a,b}(x)$. Tako kot v $\mathbb{Z}$ zdaj definiramo deljivost polinomov.

**Definicija 2.1** (Deljivost)**.** Polinom $a(x)$ je deljiv s polinomom $b(x)$, če in samo če je $r_{a,b}(x) = 0$. Povedano drugače, $b(x)|a(x) \iff \exists q(x) \in \mathbb{F}[x] : a(x) = b(x) \cdot q(x)$.

Iz tega sledi, da so stopnje deliteljev neničelnega polinoma $a(x)$ manjše ali enake $d(a(x))$, polinom $a(x) = 0$ pa delijo vsi $b(x) \in \mathbb{F}[x]$. Opazimo še, da če $b(x)|a(x)$, potem $c \cdot b(x)|a(x)$ za vse $c \in \mathbb{F} - \{0\}$ – torej za vse $c$, ki imajo multiplikativni inverz v $\mathbb{F}[x]$, podobno kot v $\mathbb{Z}$, kjer sta "možna $c$-ja", torej $c$-ja z multiplikativnim inverzom, $\pm 1$. Vsi polinomi $a(x)$ so deljivi z vsemi takimi $c$ ter s $c \cdot a(x)$.

Do zdaj smo ob iskanju dobrih definicij za najpreprostejše operacije v $\mathbb{F}[x]$ našli veliko analogij med to množico in $\mathbb{Z}$, zato bi bilo verjetno pametno s tem nadaljevati. V tem duhu si zdaj oglejmo gcd oz. **največji skupni delitelj** dveh polinomov.

**Definicija 2.2** (Največji skupni delitelj polinomov)**.** Za dva polinoma $a(x), b(x)$, ne oba ničelna, definiramo $\gcd(a(x), b(x))$ kot množico tistih polinomov $p(x)$, ki sami delijo $a(x)$ in $b(x)$, poleg tega pa so deljivi z vsemi polinomi, ki delijo $a(x)$ in $b(x)$.

**Izrek 2.2** (Obstoj in (skoraj) enoličnost gcd-ja)**.** *Izkaže se, da zgornja množica ni prazna, in da so vsi elementi te množice oblike $c \cdot p(x)$ za vse neničelne konstantne polinome $c$, za nek fiksen $p(x)$.*[3] *(Zato je običajno pisati kar $\gcd(a(x), b(x)) = p(x)$, kljub temu da ta enakost v resnici ni smiselna, ker enači množico z enim polinomom).*

*Dokaz.* Ideja je enaka dokazu analogne izjave za $\mathbb{Z}$. Ključna izjava je sledeča: če $b(x) \neq 0$, je množica skupnih deliteljev polinomov $a(x)$ in $b(x)$ enaka množici skupnih deliteljev polinomov $r_{a,b}(x)$ in $b(x)$:

$$(p(x)\big|a(x) \wedge p(x)\big|b(x)) \iff (p(x)\big|a(x) - q_{a,b}(x) \cdot b(x) = r_{a,b}(x) \wedge p(x)\big|b(x)).$$

Torej imamo $\gcd(a(x), b(x)) = \gcd(r_{a,b}(x), b(x)) = \gcd(b(x), r_{a,b}(x))$.

Brez izgube splošnosti naj bo torej $d(a(x)) > d(b(x))$ (v primeru enakosti stopenj enkrat uporabimo zgornjo enakost). Potem lahko z večkratno uporabo te enakosti reduciramo računanje $\gcd(a(x), b(x))$ na računanje $\gcd(a_k(x), b_k(x))$, kjer so $a_0(x) = a(x),\ b_0(x) = b(x),\ a_{k+1}(x) = b_k(x)$ in $b_{k+1}(x) = r_{a_k,b_k}(x)$. To zaporedje lahko rekurzivno definiramo do prvega $k$-ja, kjer je $b_k(x) = 0$ – naj

[3] Seveda ni važno, kateri $p(x)$ iz množice izberemo kot ta "bazni element".

bo to $k_0$. Ampak ker velja neenakost $d(b_{k+1}(x)) = d(r_{a_k,b_k}(x)) < d(b_k(x))$, je zaporedje stopenj $b_k(x)$ strogo padajoče! Iz tega sledi, da nujno po končno mnogo korakih (največ $d(b_0(x)) + 1$)[4] dosežemo $b_k(x) = 0$, torej $k_0$ zares obstaja in je končen. A ker vsak korak ohrani gcd, imamo $\gcd(a(x), b(x)) = \gcd(a_{k_0}(x), b_{k_0}(x)) = \gcd(a_{k_0}(x), 0) = a_{k_0}(x)$, kjer je zadnja enakost posledica dejstva, da je $\gcd(a_{k_0}(x), 0)$ množica takih deliteljev $a_{k_0}(x)$-a, ki so deljivi z vsemi delitelji $a_{k_0}(x)$-a. Sledi, da morajo biti deljivi tudi z $a_{k_0}(x)$-om samim, zato morajo imeti stopnjo natanko $d(a_{k_0}(x))$. A če tak delitelj označimo z $p(x)$, mora veljati $a_{k_0}(x) = c \cdot p(x)$ za nek neničelni konstantni $c$, torej so vsi iskani delitelji res oblike $c \cdot a_{k_0}(x)$ in smo končali. □

V resnici nam ta dokaz pove še več! Najprej opazimo, da je zgornja definicija $\gcd(a(x), b(x))$ zares ekvivalentna tisti, da je to največji (po stopnji) skupni delitelj $a(x)$-a in $b(x)$-a, saj so njuni skupni delitelji natanko delitelji $a_{k_0}(x)$-a. In še nekaj. Upam, da se spomniš Bézoutove leme iz teorije števil. Ta pravi, da za vse $x, y \in \mathbb{Z}$ obstajata $a, b \in \mathbb{Z}$, da je $ax + by = \gcd(x, y)$. In kot (bi moralo biti) pričakovano, analogno velja tudi za polinome:

**Izrek 2.3** (Bézoutova lema za polinome)**.** *Za vsaka dva polinoma $a(x), b(x) \in \mathbb{F}[x]$, ki nista oba 0, obstajata polinoma $p(x), q(x) \in \mathbb{F}[x]$, da je $p(x)a(x) + q(x)b(x) = \gcd(a(x), b(x))$.*

*Dokaz.* V zgornjem dokazu sproti beležiš izraze $a_k(x)$ in $b_k(x)$. V vsakem koraku ostaneta linearni kombinaciji $a(x)$-a in $b(x)$-a. Konec. □

Potem je očitno tudi, da so elementi množice $p(x)a(x) + q(x)b(x)$, kjer sta $p(x), q(x) \in \mathbb{F}[x]$ poljubna, natanko tisti polinomi, ki so deljivi z $\gcd(a(x), b(x))$. Iz tega z lahkoto sledijo uporabne stvari, kot na primer $\gcd(a(x), b(x) \cdot c(x)) = 1 \iff (\gcd(a(x), b(x)) = 1 \wedge \gcd(a(x), c(x)) = 1)$. Ta primer, ko je gcd dveh polinomov enak 1, je posebej pomemben, zato takim parom pravimo **tuji**.

Z malo več truda lahko dokažemo še, da lahko izberemo taka polinoma $p(x), q(x)$, da sta ali $p(x) = 1, q(x) = 0$, ali $p(x) = 0, q(x) = 1$, ali pa $d(p(x)) < d(b(x)) - d(\gcd(a(x), b(x)))$ in $d(q(x)) < d(a(x)) - d(\gcd(a(x), b(x)))$ (tega nisem nikoli videl v uporabi ampak... velja).

# 3 $p$

Zanima nas "multiplikativna struktura" naše množice. Zato bi bilo vredno raziskati možnost neke vzporednice osnovnega izreka aritmetike (obstoja enoličnega razcepa na "praštevila"). Za to najprej definiramo **nerazcepne polinome**.

[4] Zanimivo... računanje gcd-ja v celih številih je najpočasnejše za pare sosednjih Fibonaccijevih števil, kjer je potrebnih približno $\log_\varphi(F_n)$ korakov. To se torej sklada s prejšnjo heuristiko, da je stopnja logaritem "prave velikosti"! V obeh primerih namreč za izračun $\gcd(a, b)$ rabimo reda velikosti $\log(\min(\text{velikost}(a), \text{velikost}(b)))$ deljenj z ostanki.

**Definicija 3.1.** Nerazcepni polinomi so nekonstantni polinomi $p(x) \in \mathbb{F}[x]$, za katere za vse $a(x), b(x) \in \mathbb{F}[x]$ velja $p(x) \big| a(x) \cdot b(x) \implies (p(x) \big| a(x) \vee p(x) \big| b(x))$. Ekvivalentno, to so nekonstantni polinomi, katerih delitelji so natanko polinomi oblike $c$ in $c \cdot p(x)$ za neničelne konstantne $c$. Še ekvivalentno, gre za nekonstantne polinome, ki so tuji natanko tistim polinomom, ki niso z njimi deljivi. Za vajo dokaži te ekvivalence! (2. $\iff$ 3. je lažja od 1. $\iff$ 2.)

Polinom $a(x) \in \mathbb{F}[x]$ je torej razcepen, če in samo če ga lahko zapišemo kot $a(x) = b(x) \cdot c(x)$ za dva nekonstanta polinoma $b(x), c(x) \in \mathbb{F}[x]$. Ta nekonstantnost pomeni, da sta stopnji $d(b(x)), d(c(x)) < d(a(x))$. Poleg tega so očitno vsi linearni (tj. s stopnjo 1) polinomi nerazcepni. Iz tega sledi, da lahko rekurzivno vsak polinom $a(x)$ zapišemo kot produkt nerazcepnih polinomov:

$$a(x) = \prod_{i=1}^{k} p_i(x)^{e_i};\ e_i \in \mathbb{N}\ \ \forall 1 \leq i \leq k,\ \gcd(p_i(x), p_j(x)) = 1\ \ \forall 1 \leq i < j \leq k.$$

Želeli bi, da je ta zapis enolično določen (do preureditve $p_i(x)$-ov in njihovega množenja z neničelno konstanto). Na srečo se to da z lahkoto dokazati.

*Dokaz.* Denimo, da lahko $a(x)$ zapišemo na dva različna načina

$$a(x) = \prod_{i=1}^{k} p_i(x)^{e_i} \prod_{i=1}^{l} q_i(x)^{f_i} = \prod_{i=1}^{k} p_i(x)^{e_i} \prod_{i=1}^{m} r_i(x)^{g_i},$$

kjer so $p_i(x)$ med seboj paroma tuji nerazcepni polinomi, enako velja za unijo vseh $q_i(x)$ in $r_i(x)$, ter sta $l, m \geq 1$ (po predpostavki mora biti vsaj en, a zaradi enakosti stopenj morata biti oba). Potem dobimo:

$$\prod_{i=1}^{k} p_i(x)^{e_i} \prod_{i=1}^{l} q_i(x)^{f_i} = \prod_{i=1}^{k} p_i(x)^{e_i} \prod_{i=1}^{m} r_i(x)^{g_i} \implies q_1(x) \Big| \prod_{i=1}^{m} r_i(x)^{g_i} \implies q_1(x) \big| r_j(x)$$

za nek $j$, kjer je druga implikacija posledica nerazcepnosti $q_1(x)$-a. Ker je $r_j(x)$ nerazcepen, sledi $q_1(x) = c \cdot r_j(x)$ za nek neničelni konstantni $c$, kar je protislovje. □

V splošnem je nerazcepnost družin polinomov precej težko dokazati, zato se take naloge pogosto pojavljajo na olimpijadah.[5] A če to primerjamo s celimi števili, je zanimivo, da take družine sploh obstajajo – ne obstaja nobeno "preprosto" zaporedje celih števil, ki je dokazljivo vedno praštevilsko.

[5] Žal večina metod, ki se jih uporablja pri teh nalogah, temelji na nekaterih malo zapletenejših principih (Gaussova lema in druge ideje s preslikavo v $\mathbb{F}_p[x]$ kot npr. Eisensteinov kriterij, nešteto analitskih metod, razširitve polj), zato jih bom obravnaval sproti, ko pridemo do njih.

## 4 $'$

Obstaja ena nekoliko posebna operacija, ki nam da v $\mathbb{F}[x]$ več svobode kot je imamo v $\mathbb{Z}$: odvod. Verjetno se zdi čudno uvesti odvode preden sem karkoli napisal o polinomskih funkcijah. Seveda so bili zgodovinsko najprej odkriti v kontekstu analize, a v resnici lahko odvode polinomov definiramo kot funkcijo $\mathbb{F}[x] \to \mathbb{F}[x]$, ne da bi uporabili koncept limite in podobnega. In s tako definicijo lahko delamo v večji splošnosti (torej čez vsa polja $\mathbb{F}$), hkrati pa ohranimo večino lepih aritmetičnih lastnosti odvoda. O analitičnih lastnostih več pozneje, ko bodo na vrsti specifično polinomi v $\mathbb{R}[x]$ in $\mathbb{C}[x]$.

**Definicija 4.1.** Odvod je funkcija $'\colon \mathbb{F}[x] \to \mathbb{F}[x]$, ki $p(x) = \sum_{k=0}^{m} a_k x^k$ priredi vrednost

$$p'(x) = \sum_{k=1}^{m} k a_k x^{k-1} = \sum_{k=0}^{m-1} (k+1) a_{k+1} x^k.$$

Omeniti je treba, da to lahko naredimo le, ker so cela števila elementi vseh polj (ker koeficiente množimo z njimi!). Zakaj to velja? 0, 1 in $-1$ so elementi zaradi aksiomov, zato lahko z njihovim seštevanjem dobimo podmnožico polja, ki se "obnaša enako kot $\mathbb{Z}$" (obstaja funkcija (homomorfizem), ki slika $\mathbb{Z}$ v to podmnožico, in "ohranja" operacije seštevanja in množenja. V končnih poljih sicer obstaja praštevilo $p \in \mathbb{Z}$, ki se slika v 0, a nam to tu ne bo povzročalo težav, ker ne bomo delili s celimi števili.)

Ker je ta definicija drugačna od običajne, se ne moremo zanašati na lastnosti limit za dokazovanje dejstev o odvodu. Torej je treba pravila za odvajanje izpeljati lepo počasi in algebraično. Ne beri tega, če se ti ne ljubi.

Najprej: $(p+q)'(x) = p'(x) + q'(x)$.

*Dokaz.* Naj bodo $a_k$ koeficienti $p(x)$-a, $b_k$ koeficienti $q(x)$-a, in naj bo brez izgube splošnosti $m = d(p(x)) \geq d(q(x)) = n$. In kot opomnik, koeficienti $a_k$ za $k > m$ in $b_k$ za $k > n$ so 0.

$$\begin{aligned}(p+q)'(x) &= \left(\sum_{k=0}^{m} a_k x^k + \sum_{k=0}^{n} b_k x^k\right)' = \left(\sum_{k=0}^{m} (a_k + b_k) x^k\right)' = \\ &= \sum_{k=1}^{m} k(a_k + b_k) x^{k-1} = \sum_{k=1}^{m} k a_k x^{k-1} + \sum_{k=1}^{n} k b_k x^{k-1} = \\ &= p'(x) + q'(x).\end{aligned}$$

□

Zdaj pa še $(p \cdot q)'(x) = p'(x)q(x) + p(x)q'(x)$.

*Dokaz.* Enake predpostavke kot zgoraj.

$$\begin{aligned}
(p \cdot q)'(x) &= \left( \left( \sum_{k=0}^{m} a_k x^k \right) \cdot \left( \sum_{k=0}^{n} b_k x^k \right) \right)' = \\
&= \left( \sum_{k=0}^{m+n} \left( \sum_{l=0}^{k} a_l b_{k-l} \right) x^k \right)' = \sum_{k=1}^{m+n} k \left( \sum_{l=0}^{k} a_l b_{k-l} \right) x^{k-1} = \\
&= \sum_{k=1}^{m+n} \left( \sum_{l=0}^{k} k a_l b_{k-l} \right) x^{k-1} = \sum_{k=1}^{m+n} \left( \sum_{l=0}^{k} l a_l b_{k-l} + a_l (k-l) b_{k-l} \right) x^{k-1} = \\
&= \sum_{k=1}^{m+n} \left( \sum_{l=0}^{k} l a_l b_{k-l} \right) x^{k-1} + \sum_{k=1}^{m+n} \left( \sum_{l=0}^{k} a_l (k-l) b_{k-l} \right) x^{k-1} = \\
&= p'(x)q(x) + p(x)q'(x).
\end{aligned}$$

□

Z indukcijo lahko potem dokažemo sledeča splošnejša pravila:

$$\begin{aligned}
\left( \sum_{k=1}^{i} p_k \right)'(x) &= \sum_{k=1}^{i} p_k'(x), \\
\left( \prod_{k=1}^{i} p_k \right)'(x) &= \sum_{k=1}^{i} \left( p_k'(x) \cdot \prod_{\substack{l=1 \\ l \neq k}}^{i} p_l(x) \right).
\end{aligned}$$

Omenimo tudi to, da je $d(q'(x)) = d(q(x)) - 1$ (pedantizem, ignoriraj: razen če delamo s koeficienti v končnem polju $\mathbb{F}_{p^n}$ in $p | d(q(x))$ – takrat velja $d(q'(x)) \leq d(q(x)) - 2$). Odlično. Zdaj pa odgovor na najpomembnejše vprašanje: zakaj? Zato, ker lahko z odvodi "zaznamo" kvadratne delitelje polinomov.[6]

**Izrek 4.1** (Največji skupni delitelj $a(x)$-a in $a'(x)$-a)**.** *Če zapišemo* $a(x) = \prod_{i=1}^{k} p_i(x)^{e_i}$, *kjer so* $e_i \in \mathbb{N}$ *in so* $p_i(x)$ *nerazcepni polinomi, ki so si paroma tuji, velja:*

$$\gcd(a(x), a'(x)) = \prod_{i=1}^{k} p_i(x)^{e_i - 1}.$$

*Posebej pomembna posledica tega je, da* $\gcd(a(x), a'(x)) \neq 1$, *če in samo če obstaja nek nekonstanten polinom* $b(x) \in \mathbb{F}[x]$, *katerega kvadrat deli* $a(x)$*:* $b(x)^2 | a(x)$.

*Dokaz.* Prepuščen bralcu za vajo. (Namiga: razpiši $a'(x)$. Glej maksimalen eksponent vsakega $p_i$-ja posebej.) □

[6] Z višjimi odvodi lahko zaznaš tudi kubične delitelje itd., a je to veliko redkeje uporabno.

# 5 =

Do zdaj smo polinome obravnavali kot elemente $\mathbb{F}[x]$. A razumemo jih lahko tudi kot funkcije $p : \mathbb{F} \to \mathbb{F}$. To si intuitivno predstavljamo kot vstavljanje neke specifične vrednosti $x_0 \in \mathbb{F}$ v izraz $p(x)$-a:

$$p(x_0) = \sum_{k=0}^{m} a_k x_0^k \in \mathbb{F}.$$

Najpomembnejša lastnost polinomskih funkcij čez vsa polja $\mathbb{F}$ je sledeča:

**Izrek 5.1** (Ničle $\iff$ linearni delitelji)**.** *Za polinom $p(x) \in \mathbb{F}[x]$ in element polja $\alpha \in \mathbb{F}$ velja*

$$x - \alpha \big| p(x) \iff p(\alpha) = 0,$$

*kjer leva izjava pomeni deljivost v $\mathbb{F}[x]$, desna pa vrednost polinomske funkcije v $\mathbb{F}$.*

*Dokaz.* Delimo $p(x)$ z $x-\alpha$: $p(x) = (x-\alpha)\cdot q(x) + r$, kjer je $r \in \mathbb{F}[x]$ konstanten polinom – ostanek pri deljenju. Nato vstavimo $\alpha$: $p(\alpha) = (\alpha-\alpha)\cdot q(\alpha) + r = r$. Sledi, da je ostanek pri deljenju enak $p(\alpha)$, torej je 0 natanko tedaj, ko je $p(\alpha) = 0$. □

Ta izrek je temeljna povezava med vrednostmi polinoma in polinomom samim. Iz njega lahko izpeljemo še en zelo osnoven izrek:

**Izrek 5.2** (Neničelni $p(x)$ ima največ $d(p(x))$ različnih ničel)**.** *Povedano drugače, če ima $p(x) \in \mathbb{F}[x]$ več kot $d(p(x))$ različnih ničel v $\mathbb{F}$, mora biti $p(x) = 0$.*

*Dokaz.* Naj bodo ničle našega polinoma $\alpha_1, \alpha_2, \ldots, \alpha_n$, kjer je $n > d(p(x))$. Vsaka od njih nam da nerazcepni delitelj $p(x)$-a oblike $x - \alpha_k$. Ker so si ti delitelji paroma tuji, tudi njihov produkt $(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ deli $p(x)$ (dokaži to!). A če je polinom neničelen, imajo vsi njegovi delitelji stopnjo manjšo ali enako njemu samemu. Torej je $p(x) = 0$. □

Ta izrek se pojavi v tako rekoč vsaki nalogi iz polinomov (pogosto v malo prikriti obliki, npr. da je treba najprej kakšen polinom odšteti), zato si ga je zelo pametno zapomniti. Za konec se mi zdi dobro uvesti še idejo *večkratnosti ničle*.

**Definicija 5.1.** Večkratnost ničle $\alpha$ polinoma $p(x)$ je največje število $k \in \mathbb{N}$, za katero velja $(x-\alpha)^k \big| p(x)$.

Potem lahko s skoraj enakim dokazom povemo še, da je vsota večkratnosti ničel polinoma $p(x) \neq 0$ največ $d(p(x))$. Poleg tega velja, da je $\alpha$ ničla večkratnosti $k$, če in samo če $p(\alpha) = p'(\alpha) = \cdots = p^{(k-1)}(\alpha) = 0,\ p^k(\alpha) \neq 0$. Dokaži to!

V nekaterih poljih (najbolj znano je $\mathbb{C}$) velja še več: vsota večkratnosti ničel polinoma je natanko njegova stopnja. Povedano drugače, vsak neničelen

polinom lahko tam zapišemo kot produkt linearnih faktorjev. Takim poljem pravimo *algebraično zaprta* in so zelo uporabna, tudi če imamo opravka s polinomi čez polja, ki niso algebraično zaprta, npr. $\mathbb{Q}$.

Razlog je, da lahko $\mathbb{Q}$ *razširimo* v $\mathbb{C}$: če gledamo na $\mathbb{Q}$ kot na podmnožico $\mathbb{C}$, se operacije seštevanja in množenja ujemajo. To pomeni, da do zdaj dokazana dejstva, ki temeljijo le na operacijah na koeficientih v polju, veljajo tudi, ko "prehajamo" med polji, ki imajo take vrste ujemanje[7] (glej nalogo 6.5).

# 6 Naloge

Nekaj namigov je na zadnji strani.

**Naloga 6.1.** Reši vaje v tekstu. (Dokaz izreka 2.1, ekvivalenc v definiciji 3.1, izreka 4.1, koraka v izreku 5.2 in ekvivalenco večkratnosti ničle z vrednosti odvodov po definiciji 5.1).

**Naloga 6.2.** Dokaži, da je $x^3 - 6x^2 + 12x - 18$ nerazcepen v $\mathbb{Q}[x]$.

**Naloga 6.3.** Dokaži, da lahko sod polinom $p(x) \in \mathbb{F}[x]$ ($p(x) = p(-x)\ \forall x \in \mathbb{F}$), kjer $\mathbb{F}$ ni končno polje, zapišemo kot $p(x) = r(x^2)$ za nek $r(x) \in \mathbb{F}[x]$.

**Naloga 6.4.** Razmišljaj o množici $\mathbb{R}[x] \pmod{x^2+1}$, kjer vsakemu polinomu v $\mathbb{R}[x]$ pripišemo njegov ostanek pri deljenju z $x^2+1$. Razpiši pravila za seštevanje in množenje v tej množici. Ali te na kaj spominjajo?

**Naloga 6.5.** Dokaži, da je za dva polinoma $a(x), b(x) \in \mathbb{Q}[x]$, ki nista oba 0, njun gcd v $\mathbb{Q}[x]$ enak gcd-ju v $\mathbb{C}[x]$. Dokaži, da iz tega sledi, da za vse nerazcepne (čez $\mathbb{Q}[x]$) polinome $p(x) \in \mathbb{Q}[x]$ velja, da če ima nek polinom $a(x) \in \mathbb{Q}[x]$ vsaj eno skupno ničlo v $\mathbb{C}$ s $p(x)$-om, potem $p(x) \big| a(x)$. Za konec dokaži še lahko posledico tega: nerazcepni polinomi $p(x) \in \mathbb{Q}[x]$ nimajo kompleksnih ničel z večkratnostjo $\geq 2$.

**Naloga 6.6.** Naj bodo $p(x), q(x), r(x) \in \mathbb{Q}[x]$. Dokaži, da če $x^4 + x^3 + x^2 + x + 1 \big| p(x^5) + x \cdot q(x^5) + x^2 \cdot r(x^5)$, potem $x - 1 \big| p(x)$.

**Naloga 6.7.** Poišči vse $p(x) \in \mathbb{R}[x]$, za katere je $p(x)p(x-1) = p(x^2-1)\ \forall x \in \mathbb{R}$.

**Naloga 6.8.** Najdi vse $p(x) \in \mathbb{R}[x]$, za katere je $p(x^2+1) = p(x)^2\ \forall x \in \mathbb{R}$.

**Naloga 6.9.** Najdi vse pare $p(x), q(x) \in \mathbb{Z}[x]$ s $p(q(x)) = x^{1585} + 4x + 7$.

**Naloga 6.10.** Naj imata $p(x), q(x) \in \mathbb{C}[x]$ vodilni koeficient enak 1 in $p(p(x)) = q(q(x))$. Dokaži, da je $p(x) = q(x)$.

**Naloga 6.11.** Naj so $p(x), q(x), r(x) \in \mathbb{R}[x]$ taki, da je $p(q(x)) + p(r(x))$ konstanta. Dokaži, da je eden od $p(x)$ in $q(x) + r(x)$ konstanta.

**Naloga 6.12.** Najdi vse polinome $p(x) \in \mathbb{R}[x]$, za katere je $p(a-b) + p(b-c) + p(c-a) = 2p(a+b+c)$ za vse $a, b, c \in \mathbb{R}$, ki zadoščajo $ab + bc + ca = 0$.

[7] Temu ujemanju se reče homomorfizem. Je funkcija $\phi : \mathbb{F}_1 \to \mathbb{F}_2$, za katero velja $\phi(a+b) = \phi(a) + \phi(b)$ in $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ za poljubna $a, b \in \mathbb{F}_1$. Seštevanje in množenje v oklepajih seveda pomenita seštevanje in množenje v $\mathbb{F}_1$, tista izven oklepajev pa v $\mathbb{F}_2$.

Namigi:
6.1.: V tekstu.
6.2.: Kakšne so lahko stopnje faktorjev kubičnega polinoma?
6.3.: Konstruiraj polinom z $\infty$ ničlami. Glej koeficiente.
6.4.: $p(x) = (x^2 + 1) \cdot q(x) + ax + b$.
6.5.: Poglej si dokaz/algoritem za računanje gcd-ja.
6.6.: Malo troll naloga. Katera kompleksna števila bi bilo lepo vstaviti?
6.7.: Glej kompleksne ničle.
6.8.: Loči na sod in lih primer. V sodem primeru naredi pametno substitucijo.
6.9.: Glej koeficiente visokih potenc $x$-a.
6.10.: Glej koeficiente visokih potenc $x$-a.
6.11.: Sori, Genčev problem. Kot pri prejšnji nalogi, razpisuj koeficiente.
6.12.: Konstruiraj lepo družino takih $a, b, c$ in glej vodilne koeficiente.