Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 10

Polinomi - uvod

Polinomi - podsećanje

Iz sedmog razreda osnovne škole:

- **Konstante ili koeficijenti** su brojevi i simboli koji predstavljaju prozivoljan broj (npr. $0, 1, \sqrt{3}, a$), a **promenljive** su simboli koji mogu biti zamenjeni bilo kojim brojem (npr. t, x, y, z)
- **Monomi** su izrazi sastavljeni od brojeva, promenljivih, kao i izraza dobijenih njihovim množenjem (npr. $3x, ax^2, 2ax^3$)
- **Polinomi** su algebarski izrazi sastavljeni od konstanti, promenljivih i znakova sabiranja, oduzimanja i množenja (npr. $2(x + x^2), 2x(1 + x)$)
- Svaki polinom se može transformisati u **sređen oblik polinoma** sabiranjem njegovih sličnih monoma (npr. $2x^2 + 2x$). **Stepen polinoma**
- **Sabiranje i množenje polinoma**
- **Rastavljanje polinoma na činioce**

Iz srednje škole:

- **Deljenje polinoma**
- **Koreni kvadratnog polinoma i Vijetove formule**

Polinomi - nastavak

Zaključak: Svaki polinom može se zapisati u sređenom obliku kao

$$a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n$$

gde je x promenljiva, a $a_0, \ldots, a_n$ su konstante (tj. koeficijenti).

Pitanje: Iz kog skupa su te konstante? Takođe, pošto pri sređivanju polinoma i konstante želimo da sabiramo i množimo, koje osobine operacija na tom skupu želimo da imamo? Prsten? Domen integriteta? Polje?

Odgovor: U osnovnoj i srednjoj školi ste radili sa polinomima nad poljima $(\mathbb{R}, +, \cdot)$ i $(\mathbb{C}, +, \cdot)$. Mi ćemo sada izučavati polinome nad proizvoljnim poljima.

Zašto se baviti polinomima?

- Pomoću polinoma definišemo polinomske funkcije
- Polinomske funkcije su "lepe" jer za računanje koristimo samo osnovne računske operacije
- Mnoge druge funkcije mogu se aproksimirati pomoću polinomskih funkcija
- Polinomske funkcije se pojavljuju u mnogim problemima iz raznih naučnih oblasti
- Pomoću polinoma nad konačnim poljima $(\mathbb{Z}_p, +, \cdot)$ možemo kostruisati polja sa p^n elemenata, tj. sva ostala konačna polja (koja se koriste u, npr. kriptografiji i teoriji kodovanja)

Polinomi nad proizvoljnim poljima

Definicija polinoma

Definicija

Neka je $(F, +, \cdot)$ polje. Skup svih polinoma $F[x]$ nad poljem F s proizvoljnom promenljivom x je dat sa:

1. *Konstante i promenljiva x su polinomi nad poljem F;*
2. *Ako su $p(x)$ i $q(x)$ polinomi nad poljem F tada su to i $(p(x) + q(x))$ i $(p(x) \cdot q(x))$;*
3. *Polinomi se dobijaju samo konačnim brojem primena prethodna dva pravila,*

pri čemu su operacije $+$ i $\cdot$ na skupu polinoma $F[x]$ takve da su:

- *asocijativne, komutativne i važi distributivni zakon $\cdot$ prema $+$;*
- *$+$ i $\cdot$ na skupu F jesu restrikcije od $+$ i $\cdot$ na $F[x]$;*
- *neutralni elementi su jednica 1 i nula 0 iz polja F (0 je neutralni za sabiranje, 1 je neutralni za množenje polinoma);*
- *inverzni za polinom $p(x)$ u odnosu na sabiranje polinoma je polinom $-p(x)$.*

Kanonski oblik polinoma

Iz definicije polinoma sledi:

Teorema (Kanonski oblik polinoma)

Svaki polinom $p(x)$ iz $F[x]$, sem nula polinoma 0, može se zapisati u obliku

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

gde su $a_n, \ldots, a_0 \in F$ jedinstveni i $a_n \neq 0$.

Napomena

Po definiciji, uzimaćemo da je $x^0 = 1$, tj. jedinica polja F.

Teorema (Jednakost polinoma)

U skupu $F[x]$ polinomi $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, sa $a_n \neq 0$, i $q(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$, sa $b_m \neq 0$, su jednaki akko je $n = m$ i $a_k = b_k$ za sve $k \in \{0, \ldots, n\}$.

Stepen polinoma. Sabiranje polinoma.

Definicija (Stepen polinoma)

Ako je $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, *sa* $a_n \neq 0$, *tada kažemo da je stepen polinoma* $p(x)$ *nenegativan ceo broj* n *i pišemo* $deg(p(x)) = n$. *Stepen nula polinoma* $p(x) = 0$ *nije definisan.*

Primeti: Ako je $p(x) = a_0 \neq 0$ tada je $deg(p(x)) = 0$.

Primer (Sabiranje polinoma)

Ako su $p(x) = 2x^2 + x + 2, q(x) = -x + 2$ *i* $r(x) = -2x^2 + 1$ *nad poljem* $\mathbb{R}$, *tada je*

$$p(x) + q(x) = (2x^2 + x + 2) + (-x + 2) = 2x^2 + 4$$
$$p(x) + r(x) = (2x^2 + x + 2) + (-2x^2 + 1) = x + 3$$

Primeti: Ako je $deg(p(x)) = n$ i $deg(q(x)) = m$ tada:

- za $n \neq m$ važi $deg(p(x) + q(x)) = max\{n, m\}$
- za $n = m$ važi $0 \leq deg(p(x) + q(x)) \leq n$ ili $deg(p(x) + q(x))$ nije definisan

Množenje polinoma

Teorema (Množenje)

Proizvod nenula polinoma $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ *i* $q(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ *jeste polinom* $p(x)q(x)$ *koji je stepena* $deg(p(x)q(x)) = n + m$ *čiji su koeficijenti uz* x^k *jednaki sa* $a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0$, *za* $k \in \{0, \ldots, n+m\}$.

Primer

Ako su $p(x) = 2x^2 + x + 2$ *i* $q(x) = -x + 2$ *polinomi nad* $\mathbb{R}$, *tada*

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

Teorema

Ako su $p(x)$ *i* $q(x)$ *nenula polinomni nad poljem* F, *tada je* $p(x)q(x) \neq 0$.

Dokaz

Ako je $deg(p(x)) = n$, *gde je* $a_n \neq 0$ *koeficijent uz* x^n, *i* $deg(q(x)) = m$, *gde je* $b_m \neq 0$ *koeficijent uz* x^m, *tada je* $a_n b_m$ *koeficijent uz* x^{n+m} *u polinomu* $p(x)q(x)$ *i važi* $a_n b_m \neq 0$ *jer u polju* F *nema delitelja nule.*

Domen integriteta polinoma

Teorema

Ako je $(F, +, \cdot)$ polje tada je $(F[x], +, \cdot)$ domen integriteta.

Dokaz

Po definiciji sabiranje i množenje polinoma jesu zatvoreni, asocijativni i komutativni. Takođe, u definiciji polinoma je dato da su neutralni za $+$ i $\cdot$ nula i jednica iz polja F i da je inverzni za polinom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ u odnosu na sabiranje $-p(x) = -a_n x^n - a_{n-1} x^{n-1} - \ldots - a_1 x - a_0$. Konačno, $(F[x], +, \cdot)$ nema delitelje nule na osnovu prethodne teoreme.

Napomena

Ako je $deg(p(x)) > 0$ tada je $p(x)q(x) \neq 1$ za svaki polinom $q(x)$ jer:

- *$deg(p(x)q(x)) \geq deg(p(x)) > 0$, za $q(x) \neq 0$*
- *$p(x)q(x) = 0$, za $q(x) = 0$*

Dakle, $(F[x], +, \cdot)$ jeste domen integriteta i nije polje - kao i $(\mathbb{Z}, +, \cdot)$.

Deljenje polinoma

Deljenje u domenu integriteta

Primetimo: Domeni integriteta koji nisu polja su $(\mathbb{Z}, +, \cdot)$ i $(F[x], +, \cdot)$. Ove strukture nemaju inverzne elemente u odnosu na množenje, tj. ne možemo uvek da delimo. Ali, možemo da delimo da ostatkom.

Primer

U $(\mathbb{Z}, +, \cdot)$ *i* $(\mathbb{R}[x], +, \cdot)$ *imamo:*

$$\begin{array}{r|l} 835 & :3 = 278 \\ \hline -6 & \\ \hline 23 & \\ -21 & \\ \hline 25 & \\ -24 & \\ \hline 1 & \end{array}$$

$$\begin{array}{r|l} (2x^3 - x^2 + 5x) & : (x-1) = 2x^2 + x + 6 \\ \hline -(2x^3 - 2x^2) & \\ \hline x^2 + 5x & \\ -(x^2 - x) & \\ \hline 6x & \\ -(6x - 6) & \\ \hline 6 & \end{array}$$

Deljenje polinoma

Teorema (o deljenju polinoma)

Za svaka dva $s(x)$ i $t(x) \neq 0$ polinoma iz $F[x]$ postoje jedinstveni polinomi $q(x)$ i $r(x)$ iz $F[x]$ takvi da je

$$s(x) = q(x)t(x) + r(x) \qquad \textit{odnosno} \qquad \frac{s(x)}{t(x)} = q(x) + \frac{r(x)}{t(x)},$$

pri čemu je $r(x) = 0$ ili $deg(r(x)) < deg(t(x))$.

Hornerova shema

Primer

Na jednom od prethodnih slajdova smo delili $2x^3 - x^2 + 5x \in \mathbb{R}[x]$ *polinomom* $x - 1$ *i dobili količnik* $2x^2 + x + 6$ *i ostatak* 6. *Ovo se lakše može zapisati pomoću Hornerove sheme.*

Teorema (Hornerova shema)

Deljenje polinoma $a_n x^n + a_{n-1}x^{n-1} \ldots + a_1 x + a_0$ *polinomom* $x - \alpha$ *može se kraće predstaviti pomoću sheme*

	x^n	x^{n-1}	x^{n-2}	$\ldots$	x^1	x^0	r
	a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0	
α		a_n	$\alpha b_{n-1} + a_{n-1}$	$\ldots$	$\alpha b_2 + a_2$	$\alpha b_1 + a_1$	$\alpha b_0 + a_0$
		$\|\|$	$\|\|$	$\ldots$	$\|\|$	$\|\|$	$\|\|$
		b_{n-1}	b_{n-2}	$\ldots$	b_1	b_0	r

gde je količnik $Q = b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$, *a ostatak je* r.

Deljivost polinoma

Podsećanje: Na skupu $\mathbb{Z}$ relacija deli $|$ je data sa $t \mid s$ akko $s = qt$. Ako $t \mid s$ tada kažemo da je t faktor od s.

Definicija

Polinom $t(x)$ deli polinom $s(x)$ (oba iz $F[x]$), u oznaci $t(x) \mid s(x)$, ako postoji $q(x) \in F[x]$ takav da je $s(x) = q(x)t(x)$. Ako $t(x) \mid s(x)$ tada kažemo da je $t(x)$ faktor od $s(x)$.

Teorema

Neka su $t(x), s(x), r(x) \in F[x]$. Tada važi:

1. $t(x) \mid t(x)$ *(Refleksivnost)*
2. $(t(x) \mid s(x) \wedge s(x) \mid r(x)) \Rightarrow t(x) \mid r(x)$ *(Tranzitivnost)*
3. $(t(x) \mid s(x) \wedge s(x) \mid t(x)) \Rightarrow (\exists a \in F) t(x) = a \cdot s(x)$ *("Zamalo" antisimetričnost)*
4. $(t(x) \mid s(x) \wedge t(x) \mid r(x)) \Rightarrow t(x) \mid s(x) + r(x)$
5. $(t(x) \mid s(x) \wedge t(x) \mid r(x)) \Rightarrow t(x) \mid s(x)r(x)$

Svodljivost i nesvodljivost polinoma

Podsećanje: Prirodan broj je **složen** ako je jednak proizvodu dva prirodna broja manja od njega. Broj je **prost** ako deljiv samo sa samim sobom i sa 1. Broj 1 nije ni prost ni složen.

Definicija (Svodljivi polinomi)

Polinom $p(x) \in F[x]$ je svodljiv nad poljem F akko je jednak proizvodu dva polinoma stepena nižih od njegovog.

Definicija (Nesvodljivi polinomi)

Polinom $p(x) \in F[x]$ je nesvodiljiv nad poljem F ako je stepena većeg od nule i ako nije svodljiv, tj. ako nije deljiv polinomom stepena većeg od nule a manjeg od njegovog stepena.

Napomena (Konstante nisu ni svodljive ni nesvodljive)

Nula polinom i polinomi stepena nula nisu ni svodljivi ni nesvodljivi.

Primeri svodljivih i nesvodljivih polinoma

- Polinom $p(x) = 2$ nije ni svodljiv ni nesvodljiv
- Polinom $p(x) = 2x + 2$ je nesvodljiv nad poljem $\mathbb{R}$ (i nad svakim drugim, jer je prvog stepena)
- Primeti da nad $\mathbb{R}$ važi $p(x) = 2x + 2 = 2(x + 1)$, ali za svodljivost $p(x)$ oba faktora moraju biti stepena nižeg od $p(x)$, a to implicira da ni jedan ne može biti konstanta
- Polinom $p(x) = x^2 + 2x + 1$ je svodljiv nad poljem $\mathbb{R}$ jer je $p(x) = (x + 1)(x + 1)$
- Polinom $p(x) = x^2 - 2$ je nesvodljiv nad poljem $\mathbb{Q}$, a svodljiv nad $\mathbb{R}$
- Više o svodljivosti nakon Bezuove teoreme

Najveći zajednički delilac (*NZD*)

Podsećanje: Za cele brojeve $NZD(s,t) = w$ akko $w \mid s$ i $w \mid t$ i za svaki w_1 ceo broj takav da $w_1 \mid s$ i $w_1 \mid t$, sledi $w_1 \mid w$.

Definicija

Za polinome $s(x), t(x) \in F[x]$, *imamo* $NZD(s(x), t(x)) = w(x) \in F[x]$ *akko*

1. $w(x) \mid s(x)$ *i* $w(x) \mid t(x)$ *i*
2. *za svaki* $w_1(x) \in F[x]$ *takav da* $w_1(x) \mid s(x)$ *i* $w_1(x) \mid t(x)$, *sledi* $w_1(x) \mid w(x)$.

Primer

Za $s(x) = a(x-1)^2(x+2)(x-3)^4x^7$ *i* $t(x) = b(x+1)^2(x-1)^3x^5$ *imamo*

$$NZD(s(x), t(x)) = c(x-1)^2x^5$$

za bilo koje a, b, c *iz polja nad kojim se polinomi posmatraju.*

Uzajamno prosti polinomi

Podsećanje: Celi brojevi s i t su uzajamno prosti ako je $NZD(s,t) = 1$, tj. nemaju zajedničke (proste) faktore različite od 1 ili -1.

Definicija

Polinomi $s(x), t(x) \in F[x]$ su **uzajamno prosti** *ako je $NZD(s(x), t(x)) = a$, gde je $a \in F \setminus \{0\}$. Odnosno, $s(x)$ i $t(x)$ su uzajamno prosti ako nemaju zajedničke faktore različite od konstanti.*

Definicija

Kažemo da je polinom $p(x) \in F[x]$ **normalizovan** *ako mu je vodeći koeficijent jednak jedinici polja F.*

Primer

U $\mathbb{R}[x]$ normalizovan je polinom $x^2 + 1$, dok $2x^2 + 2$ nije.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\underline{106} = 2 \cdot \underline{45} + 16$$

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\underline{106} = 2 \cdot \underline{45} + 16$$
$$\underline{45} = 2 \cdot \underline{16} + 13$$

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{aligned} \underline{106} &= 2 \cdot \underline{45} + 16 \\ \underline{45} &= 2 \cdot \underline{16} + 13 \\ \underline{16} &= 1 \cdot \underline{13} + 3 \end{aligned}$$

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{aligned} \underline{106} &= 2 \cdot \underline{45} + 16 \\ \underline{45} &= 2 \cdot \underline{16} + 13 \\ \underline{16} &= 1 \cdot \underline{13} + 3 \\ \underline{13} &= 4 \cdot \underline{3} + 1 \\ \underline{3} &= 3 \cdot \underline{1} + 0 \end{aligned}$$

$NZD(45, 106) = 1$, *tj. brojevi su uzajamno prosti.*

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{aligned} \underline{106} &= 2 \cdot \underline{45} + 16 \\ \underline{45} &= 2 \cdot \underline{16} + 13 \\ \underline{16} &= 1 \cdot \underline{13} + 3 \\ \underline{13} &= 4 \cdot \underline{3} + 1 \\ \underline{3} &= 3 \cdot \underline{1} + 0 \end{aligned}$$

$NZD(45, 106) = 1$, *tj. brojevi su uzajamno prosti.*

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

$$\underline{x^3 - 2x + 1} = x\underline{(x^2 - 1)} + (-x + 1)$$

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{aligned} \underline{106} &= 2 \cdot \underline{45} + 16 \\ \underline{45} &= 2 \cdot \underline{16} + 13 \\ \underline{16} &= 1 \cdot \underline{13} + 3 \\ \underline{13} &= 4 \cdot \underline{3} + 1 \\ \underline{3} &= 3 \cdot \underline{1} + 0 \end{aligned}$$

$NZD(45, 106) = 1$, *tj. brojevi su uzajamno prosti.*

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

$$\begin{aligned} \underline{x^3 - 2x + 1} &= x\underline{(x^2 - 1)} + (-x + 1) \\ \underline{x^2 - 1} &= -x\underline{(-x + 1)} + (x - 1) \end{aligned}$$

Euklidov algoritam

Pitanje: Kako proveriti da li su dva polinoma uzajamno prosta? Tj. kako naći *NZD*?
Odgovor: Pomoću Euklidovog algoritma.

Primer

Izračunaj $NZD(45, 106)$.

$$\begin{aligned} \underline{106} &= 2 \cdot \underline{45} + 16 \\ \underline{45} &= 2 \cdot \underline{16} + 13 \\ \underline{16} &= 1 \cdot \underline{13} + 3 \\ \underline{13} &= 4 \cdot \underline{3} + 1 \\ \underline{3} &= 3 \cdot \underline{1} + 0 \end{aligned}$$

$NZD(45, 106) = 1$, *tj. brojevi su uzajamno prosti.*

Izračunaj $NZD(x^3 - 2x + 1, x^2 - 1)$.

$$\begin{aligned} \underline{x^3 - 2x + 1} &= x\underline{(x^2 - 1)} + (-x + 1) \\ \underline{x^2 - 1} &= -x\underline{(-x + 1)} + (x - 1) \\ \underline{-x + 1} &= (-1)\underline{(x - 1)} + 0 \end{aligned}$$

$NZD(x^3 + 2x + 1, x^2 + 1) = x - 1$, *tj. polinomi nisu uzajamno prosti.*

Jedinstvenost normalizovanog *NZD*-a

Podsećanje: Za $s, t \in \mathbb{N}$ postoji tačno jedan $w \in \mathbb{N}$ takav da je $NZD(s,t) = w$ koji se dobija iz Euklidovog algoritma.

Teorema

Za polinome $s(x), t(x) \in F[x]$, gde je $s(x) \neq 0$ ili $t(x) \neq 0$, postoji tačno jedan normalizovan $w(x) \in F[x]$ takav da je $NZD(s(x), t(x)) = w(x)$, koji se dobija iz Euklidovog algoritma.

Malo istorije

Antička Grčka

Napomena

Polinomi su izrazi, a njima odgovarajuće funkcije se zovu polinomske funkcije.

Počeci:

- U Staroj Grčkoj (V vek p.n.e.) **Pitagora i pitagorejci** su rešavali jednačine oblika $ax = x^2$ geometrjiski - traženjem preseka prave i parabole;
- Tri najznačajnija matematička problema anitičke Grčke: **Duplikacija kocke**, **Trisekcija ugla** i **Kvadratura kruga** - traže se konstrukcije samo pomoću lenjira i šestara (npr. Arhimed je rešio kvadraturu kruga koristeći spirale);
- Savremena matematička notacija se pojavljuje mnogo kasnije, ali dva od tri problema prevedena na jezik današnje matematike su zapravo kubne jednačine
  - **Duplikacija kocke:** $2x^3 - a^3 = 0$
  - **Trisekcija ugla:** $\sin(3\alpha) = 3\sin\alpha - 4\sin^3\alpha$, odnosno $4x^3 - 3x + a = 0$

Srednji vek - Kuća mudrosti u Bagdadu

- **Al Horezmi** početkom *IX* veka objavljuje traktat o algebri pod nazivom *Hisab al džabr bal mukabala* - knjiga o svođenju i uravnotežavanju
- U prevodima je *al džabr* postao **algebra**, a od imena Al Horezmi nastao je naziv **algoritmi**
- U samoj knjizi Al Horezmi daje sistematičan pregled rešavanja **kvadratnih jednačina**, tj. $ax^2 + bx + c = 0$,
- pri čemu je koristio **indijske brojeve**, koji su u Evropu stigli preko Al Horezmija i drugih arapskih matematičara, odatle (pogrešan) naziv **arapski brojevi**

Renesansa - kubna jednačina

Kubna jednačina $ax^3 + bx^2 + cx + d = 0$.

- **del Fero** je u *XV* veku u Bolonji pronašao rešenja kubne jednačine
- Nakon njega i **Tartalja**, koji je svoje rešenje rekao **Kardanu** (koji se zakleo da će tajnu čuvati) i koji ih objavljuje u knjizi *Ars Magna*
- Danas su rešenja poznata kao **Kardanove formule**
- S tim što je u Ars Magni Kardano lepo opisao čitav istorijat
- Kardanov učenik **Ferari** pronalazi rešenja jednačine četvrtog stepena

Polinomi petog stepena i većeg. Nastanak teorije grupa

- Početkom *XIX* veka **Ervaist Galoa** uvodi pojam **grupe** i posmatra permutacije korena polinoma kroz strukturu grupe
- U slično vreme **Nils Abel**, koristeći permutacije korena polinoma, pokazuje da se nesvodljiva jednačina trećeg stepena ne može rešiti u "kvadraturama" i da se jednačine petog i većeg stepena ne mogu rešiti u "radikalima" (pomoću korena). Dakle:
  - Abel je pokazao da se jednačine petog i većeg stepena ne mogu rešiti kao jednačine stepena $2, 3$ i 4 koristeći osnovne računske operacije i koren
  - Abel je pokazao da duplikacija kocke i trisekcija ugla (koristeći samo šestar i lenjir) nije moguća
- Inače, krajem *XIX* veka, Lindeman pokazuje da ni kvadratura kruga nije moguća jer je broj π transcedentan (iracionalan i nije koren polinoma sa racionalnim koeficijentima)

Polinomske funkcije

Polinomske funkcije

Napomena: Polinomi su izrazi, a njima odgovarajuće funkcije se zovu polinomske funkcije.

Definicija (Polinomska funkcija)

Neka je $(F, +, \cdot)$ *polje. Ako je* $p(x) = a_n x^n + \ldots + a_1 x + a_0 \in F[x]$, *tada se funkcija* $f_p : F \to F$ *oblika*

$$f_p(x) = a_n x^n + \ldots + a_1 x + a_0$$

zove ***polinomska funkcija***. *Skup svih polinomskih funkcija nad* F *označavamo sa* $Pol(F)$.

Definicija

Za polinomske funkcije sabiranje i množenje nad poljem $(F, +, \cdot)$ *definišemo sa: za sve* $x \in F$ *i sve* $f_p, f_q \in Pol(F)$

$$(f_p + f_q)(x) = f_p(x) + f_q(x),$$

$$(f_p \cdot f_q)(x) = f_p(x) \cdot f_q(x).$$

Prsten polinomskih funkcija

Teorema

Neka je F polje. Tada je $(Pol(F), +, \cdot)$ komutativan prsten sa jedinicom.

Dokaz

Pokazujemo da je $(Pol(F), +)$ Abelova grupa.

Zatvorenost: *Neka su $f_p, f_q \in Pol(F)$. Tada su $p(x), q(x) \in F[x]$ i znamo da je $p(x) + q(x) \in F[x]$. Neka su $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ i $q(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ i neka je $n > m$ (slučaj kada je $n \leq m$ je analogan). Tada je $(f_p + f_q)(x) = f_p(x) + f_q(x) =$ $a_n x^n + \ldots + a_{m+1}x^{m+1} + (a_m + b_m)x^m \quad + \ldots + (a_1 + b_1)x + (a_0 + b_0) = f_{p+q}(x)$. Kako je $f_p + f_q = f_{p+q}$, sledi $f_p + f_q \in Pol(F)$.*

Asocijativnost i komutativnost: *Slede iz asocijativnosti i komututativnosti operacije $+$ u F.* **Neutralni i inverzni:** *$f_0 \in Pol(F)$ je neutralni element. Za funkciju $f_p \in Pol(F)$ inverzni element je $f_{-p} \in Pol(F)$.*

Analogno se dokazuje da je $(Pol(F), \cdot)$ komutativan monoid, kao i da važi distributivnost $\cdot$ prema $+$, te je $(Pol(F), +, \cdot)$ komutativan prsten sa jedinicom.

Veza između polinoma i polinomskih funkcija

Teorema

Funkcija $\psi : F[x] \to Pol(F)$ iz domena integriteta $(F[x], +, \cdot)$ u prsten $(Pol(F), +, \cdot)$, definisana sa $\psi(p(x)) = f_p(x)$, jeste sirjektivni homomorfizam.

Napomena

Pošto su polinomske funkcije definisane u svakoj tački skupa F imamo da važi

$$f_p = f_q \quad \Leftrightarrow \quad \text{za svako } x \in F : \ f_p(x) = f_q(x)$$

Ako su dva polinoma jednaka jasno je da su jednake i njihove polinomske funkcije, ali obrnuto ne mora da važi (videćemo kad budemo radili polinome nad konačnim poljima).

Koreni (nule) polinoma. Bezuov stav

Definicija

Vrednost polinoma $p(x) \in F[x]$ u tački $\alpha \in F$ jeste vrednost njegove polinomske funkcije u tački α, tj. $f_p(\alpha)$. Kažemo da je α ***koren*** *(**nula**) polinoma $p(x)$ ako je $f_p(\alpha) = 0$.*

Teorema (Bezuova)

Vrednost polinoma $p(x) \in F[x]$ u tački $\alpha \in F$ jednaka je ostatku pri deljenju polinoma $p(x)$ polinomom $x - \alpha$.

Dokaz

Na osnovu teoreme o deljenju polinoma znamo da kada delimo polinom $p(x)$ polinomom $x - \alpha$, postoje jedinstveni polinomi $q(x)$ i $r(x)$ takvi da je $r(x) = 0$ ili $deg(r(x)) < deg(x - \alpha)$ (odnosno $r(x) = c$, za neko $c \in F$), i da važi $p(x) = q(x) \cdot (x - \alpha) + r(x)$. Primenjujući homomorfizam ψ iz prethodne teoreme na poslednju jednakost dobijamo da za svako $x \in F$ važi $f_p(x) = f_q(x) \cdot (x - \alpha) + f_r(x)$, gde je $f_r(x) = c$. Ako sada uvrstimo $x = \alpha$, dobijamo $f_p(\alpha) = c$.

Koreni polinoma i faktorizacija

Iz Bezuovog stava direktno imamo sledeću posledicu.

Posledica

Polinom $x - \alpha$, za $\alpha \in F$, je faktor polinoma $p(x) \in F[x]$, odnosno $(x - \alpha) \mid p(x)$ akko je α koren polinoma $p(x)$.

Primer

Pošto za polinom $p(x) = 2x^3 + 3x^2 - 5x \in \mathbb{R}[x]$ važi $f_p(1) = 0$, tj. 1 je koren polinoma $p(x)$, sledi da je $x - 1$ faktor polinoma $p(x)$, tj. da $(x - 1) \mid p(x)$.

Definicija (Višestruki koreni)

Kažemo da je $\alpha \in F$ k-tostruki koren polinoma $p(x) \in F[x]$ ako važi $(x - \alpha)^k \mid p(x)$ i $(x - \alpha)^{k+1} \nmid p(x)$

Primer

Za polinom $p(x) = (x - 1)^3(x - 2)^4$ imamo da je 1 trostruki, a 2 četvorostruki koren.

Maksimalan broj korena polinoma

Teorema

Neka je $p(x) \in F[x]$. Ako je $\deg(p(x)) = n$, tada $p(x)$ ima najviše n korena brojeći i njihove višestrukosti.

Dokaz

Ako $p(x)$ nema korena u F dokaz je gotov, zato pretpostavimo da $p(x)$ ima bar jedan koren u F. Dokaz izvodimo indukcijom po stepenu polinoma $p(x)$:

- **Baza indukcije:** *Za $n = 0$ imamo $p(x) \in F \setminus \{0\}$, pa $p(x)$ nema korena u F. Za $n = 1$ imamo $p(x) = ax + b$, pa je jedini koren u polju $-ba^{-1}$.*
- **Indukcijska hipoteza:** *Pretpostavimo da za $\deg(p(x)) = n - 1$ polinom $p(x)$ ima najviše $n - 1$ korena.*
- **Indukcijski korak:** *Neka je $\deg(p(x)) = n$. Iz pretpostavke da $p(x)$ ima bar jedan koren α u F i posledice Bezuove teoreme imamo $p(x) = (x - \alpha)q(x)$, gde je $\deg(q(x)) = n - 1$. Na osnovu indukcijske hipoteze sledi da polinom $q(x)$ ima najviše $n - 1$ korena, odakle $p(x)$ ima najviše n korena.*

Svodljivost polinoma drugog i trećeg stepena

Teorema

Ako je $p(x) \in F[x]$ polinom drugog ili trećeg stepena, tada je $p(x)$ svodljiv nad poljem F akko ima koren u F.

Dokaz

($\Rightarrow$) *Neka je $p(x)$ svodljiv, tj. $p(x) = q(x) \cdot r(x)$, gde je $\deg(q(x)) \geq 1$ i $\deg(r(x)) \geq 1$. Ako je $\deg(p(x)) = 2$ onda $\deg(q(x)) = \deg(r(x)) = 1$, a ako je $\deg(p(x)) = 3$ tada jedan od polinoma $q(x)$ i $r(x)$ mora biti stepena 1, a drugi stepena 2. Tvrđenje sledi jer polinom prvog stepena $ax + b$ u svakom polju ima koren $-ba^{-1}$.*

($\Leftarrow$) *Neka je $p(x)$ polinom stepena 2 ili 3 i neka je α njegov koren u polju F. Iz Bezuove teoreme tada imamo $(x - \alpha) \mid p(x)$, odnosno $p(x)$ je svodljiv.*

Primeri. Svodljivost i koreni

- Polinom prvog stepena $ax + b$, sa $a \neq 0$, je nesvodljiv nad svakim poljem
- Polinom $p(x) = x^2 - 2$ je
  - svodljiv nad poljima $\mathbb{R}$ i $\mathbb{C}$ jer se može zapisati kao $(x - \sqrt{2})(x + \sqrt{2})$
  - nesvodljiv nad poljem $\mathbb{Q}$ (nema koren)
- Polinom $p(x) = x^2 + 1$ je
  - svodljiv nad poljem $\mathbb{C}$ jer se može zapisati kao $(x - i)(x + i)$
  - nesvodljiv nad poljima $\mathbb{R}$ i $\mathbb{Q}$ (nema koren)

Napomena

- *Samo za polinome stepena* 2 *i* 3 *važi da ako su svodljivi onda moraju imati koren u polju. Na primer, polinom* $x^4 + x^2 + 1$ *je svodljiv nad svim poljima, jer je* $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$, *a nema koren u, recimo,* $\mathbb{R}$ *i* $\mathbb{Q}$.
- *Za sve polinome stepena većeg od* 1 *važi da ako imaju koren onda su i svodljivi.*
- *Polinomi stepena* 1 *imaju koren u svakom polju, a nesvodljivi su nad svakim poljem.*

Jedinstvenost faktorizacije za normalizovane polinome

Podsećanje: Svaki prirodan broj se na jedinstven način može napisati kao proizvod njegovih prostih faktora (faktorisati), ako redosled faktora nije bitan. Kod brojeva kao faktor ne uzimamo u obzir 1, a kod polinoma konstante.

Teorema

Neka je polinom $P \in F[x]$ svodljiv. Tada se P može na jedinstven način napisati kao proizvod svojih nesvodljivih normalizovanih faktora i jedne konstante iz F, ako redosled faktora nije bitan.

Primer

Nad poljem $\mathbb{R}$ imamo faktorizacije
$2x^2 - 2 = 2(x+1)(x-1) = (2x+2)(x-1) = (x+1)(2x-2) = (\frac{x}{2} + \frac{1}{2})(4x-4)$.
Ako u obzir uzimamo samo normalizovane nesvodljive faktore imamo jedinstvenu faktorizaciju $2x^2 - 2 = 2(x+1)(x-1)$.

Vijetove formule

Vijetove formule

Za polinom drugog stepena $p(x) = ax^2 + bx + c$ nad proizvoljnim poljem imamo da ako su mu koreni x_1 i x_2 tada je
$ax^2 + bx + c = a(x - x_1)(x - x_2) = ax^2 - a(x_1 + x_2)x + ax_1x_2$, odakle dobijamo Vijetove formule: $x_1 + x_2 = -\frac{b}{a}$ i $x_1x_2 = \frac{c}{a}$. Ovaj rezultat može se uopštiti na polinome proizvoljnog stepena većeg od 2.

Teorema

Neka je $p(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in F[x]$ i neka su $x_1, x_2, \ldots, x_n$ svi koreni polinoma $p(x)$ (koreni se mogu ponavljati), tada važi

$$x_1 + x_2 + \ldots + x_n = -a_{n-1}a_n^{-1}$$

$$x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = a_{n-2}a_n^{-1}$$

$$\vdots$$

$$x_1x_2 \ldots x_n = (-1)^n a_0 a_n^{-1}$$

Primer

Neka je $f(x) = x^3 + ax^2 + bx + c$ polinom nad poljem $\mathbb{R}$ i neka je skup svih njegovih korena $\{1, 2\}$. Odrediti sve moguće vrednosti za a, b i c.
Rešenje. Vijetove formule za $f(x) = x^3 + ax^2 + bx + c$ glase

$$\begin{aligned} x_1 + x_2 + x_3 &= -a \\ x_1x_2 + x_1x_3 + x_2x_3 &= b \\ x_1x_2x_3 &= -c \end{aligned}$$

S obzirom da su koreni 1 i 2 imamo dve mogućnosti:

- Dvostruki koren je 1. Tada je $a = -4, b = 5, c = -2$.
- Dvostruki koren je 2. Tada je $a = -5, b = 8, c = -4$.