Algebra

Ivan Prokić

Fakultet tehničkih nauka, Novi Sad

Predavanje 13

Na prethodnom času

- Definicija polinoma nad proizvoljnim poljem
- Domen integriteta polinoma
- Deljenje polinoma
- Uzajamno prosti polinomi i *NZD*
- Euklidov algoritam

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 $(F[t], +, \cdot)$ domen integriteta polinoma nad poljem F. Posmatramo funkciju ψ koja svaki polinom $P = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$ iz $F[t]$ preslikava u polinomsku funkciju $\psi(P) : F \to F$ definisanu sa $(\forall x \in F)\psi(P)(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$. Skup svih polinomskih funkcija nad poljem F označžnačava se sa $Pol(F)$.

Definicija

Neka je $(F, +, \cdot)$ polje i neka je $F^F = \{f \mid f : F \to F\}$ skup svih funkcija nad F. Za sve $f, g \in F^F$ definišemo $f + g$ i $f \cdot g$ sa

$$(\forall x \in F)(f + g)(x) = f(x) + g(x)$$
$$(\forall x \in F)(f \cdot g)(x) = f(x) \cdot g(x)$$

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.*
  1. **Zatvorenost:** *Neka su $\psi(P), \psi(Q) \in Pol(F)$. Tada su $P, Q \in F[t]$ i znamo da je $P + Q \in F[t]$. Neka su $P = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$ i $Q = b_m t^m + b_{m-1} t^{m-1} + \ldots + b_1 t + b_0$ i neka je $n > m$ (slučaj kada je $n \leq m$ je analogan). Tada je $(\psi(P) + \psi(Q))(x) = \psi(P)(x) + \psi(Q)(x) = (a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) + (b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0) = a_n x^n + \ldots + a_{m+1} x^{m+1} + (a_m + b_m) x^m + \ldots + (a_1 + b_1) x + (a_0 + b_0) = \psi(P + Q)(x)$. Kako je $\psi(P) + \psi(Q) = \psi(P + Q)$ sledi $\psi(P) + \psi(Q) \in Pol(F)$.*
  2. **Asoc. i komut.:** *Sledi iz asoc. i komut. $+$ na skupu F^F (jer je $Pol(F) \subseteq F^F$).*
  3. **Neutralni element:** $\psi(0) \in Pol(F)$.
  4. **Inverzni elementi:** *Za $\psi(P) \in Pol(F)$ inverzni je $\psi(-P) \in Pol(F)$.*
- *$(Pol(F), \cdot)$ je komutativan monoid i distributivnost $\cdot$ prema $+$ se dokazuje analogno (ima puno pisanja).*

Veza između polinoma i polinomskih funkcija

Teorema

Funkcija $\psi : F[t] \to Pol(F)$ iz domena integriteta $(F[t], +, \cdot)$ u prsten $(Pol(F), +, \cdot)$ jeste sirjektivni homomorfizam.

Dokaz

$\psi(P) + \psi(Q) = \psi(P + Q)$ *smo pokazali u prethodnom dokazu, a* $\psi(P) \cdot \psi(Q) = \psi(P \cdot Q)$ *se pokazuje analogno (ima puno pisanja). Sirjektivnost sledi iz definicije polinomskih funkcija (za svaku funkciju iz $Pol(F)$ postoji odgovarajući polinom iz $F[t]$).*

Napomena (Nad konačnim poljima imamo delioce nule i ψ nije $1-1$)

Prsten $(Pol(F), +, \cdot)$ nije domen integriteta ako je F konačno polje. Na primer, u $Pol(\mathbb{Z}_3)$, za $f(x) = x^2 + 2$ i $g(x) = x$ imamo $(f \cdot g)(x) = x(x^2 + 2) = 0$, tj. imamo delioce nule. Generalno, ako je F polje od m elemenata, tada je $(F \setminus \{0\}, \cdot)$ grupa od $m - 1$ elemenata, pa je $x^{m-1} = 1$, odakle je $x^m = x$. Sada za $t^3, t \in \mathbb{Z}_3[t]$ imamo $\psi(t^3) = \psi(t)$, tj. ψ nije injektivna.

Koreni (nule) polinoma. Bezuov stav

Definicija

Vrednost polinoma $P \in F[t]$ u tački $\alpha \in F$ jeste vrednost njegove polinomske funkcije $\psi(P)$ u tački α. Kažemo da je α koren (nula) polinoma P ako je $\psi(P)(\alpha) = 0$.

Teorema (Bezuova)

Vrednost polinoma $P \in F[t]$ u tački $\alpha \in F$ jednaka je ostatku pri deljenju polinoma P polinomom $t - \alpha$.

Dokaz

Na osnovu teoreme o deljenju polinoma znamo da kada delimo polinom P polinomom $t - \alpha$ postoje jedinstveni Q i R polinomi takvi da je $R = 0$ ili $dg(R) < dg(t - \alpha)$ i da važi $P = Q \cdot (t - \alpha) + R$. Primenjujući ψ na poslednju jednakost dobijamo $\psi(P) = \psi(Q) \cdot \psi(t - \alpha) + \psi(R)$, odnosno da za svako $x \in F$ važi $\psi(P)(x) = \psi(Q)(x) \cdot (x - \alpha) + R$, gde je $\psi(R) = R$ jer važi $R \in F$ (jer $R = 0$ ili $dg(R) = 0$). Ako sada uvrstimo $x = \alpha$ dobijamo $\psi(P)(\alpha) = R$.

Hornerova šema

Primer

Na prošlom predavanju smo delili $2t^3 - t^2 + 5t \in \mathbb{R}[t]$ *polinomom* $t - 1$ *i dobili količnik* $2t^2 + t + 6$ *i ostatak* 6*. Ovaj ostatak je lakše dobiti iz Bezuove teoreme:* $p(1) = 2 \cdot 1^3 - 1^2 + 5 \cdot 1 = 6$.

Teorema (Hornerova šema)

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

	a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0
α	a_n	$\alpha b_{n-1} + a_{n-1}$	$\alpha b_{n-2} + a_{n-2}$	$\ldots$	$\alpha b_1 + a_1$	$\alpha b_0 + a_0$
	$\|\|$	$\|\|$	$\|\|$	$\ldots$	$\|\|$	$\|\|$
	b_{n-1}	b_{n-2}	b_{n-3}	$\ldots$	b_0	R

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

Koreni polinoma i faktorizacija

Iz Bezuovog stava direktno imamo sledeću posledicu.

Posledica

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

Primer

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

Definicija (Višestruki koreni)

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

Primer

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

Maksimalan broj korena polinoma

Teorema

Neka je $P \in F[t]$. Ako je $dg(P) = n$ tada P ima najviše n korena.

Dokaz

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

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

Polinomske funkcije nad beskonačnim poljima (1/2)

Napomena

Ranije smo pokazali da prsten $(Pol(F), +, \cdot)$ ima delitelje nule ako je F konačno polje i da ψ nije injektivna. Za beskonačna polja važi da $(Pol(F), +, \cdot)$ jeste domen integriteta i da je izomorfan sa $(F[t], +, \cdot)$. Zato ćemo nad beskonačnim poljima umesto $\psi(P)$ pisati samo P, tj. nećemo praviti razliku između polinoma i polinomskih funkcija.

Lema

Neka je F beskonačno polje. Tada za $P \in F[t]$ važi $P = 0$ akko $(\forall x \in F)\psi(P)(x) = 0$, tj. svi elementi polja su koreni polinoma P.

Dokaz

$(\Rightarrow)$: *Ako je $P = 0$ tada je $\psi(P)(\alpha) = 0$, za sve $\alpha \in F$.*

$(\Leftarrow)$: *Neka je P polinom takav da je svako $\alpha \in F$ njegov koren. Za polinom P važi $P = 0$ ili $dg(P) = n$ za $n \geq 0$. Neka je $dg(P) = n$. Tada na osnovu prethodne teoreme imamo da P može imati najviše n korena, što je u kontradikciji sa pretostavkama da su svi elementi polja F koreni polinoma P i da polje F ima beskonačno mnogo elemenata. Dakle, mora važiti $P = 0$.*

Polinomske funkcije nad beskonačnim poljima (2/2)

Teorema

Neka je F beskonačno polje. Polinomi $P, Q \in F[t]$ su jednaki akko su jednake njihove polinomske funkcije.

Dokaz

($\Rightarrow$) : *Ako je $P = Q$ tada je $\psi(P) = \psi(Q)$ jer je ψ funkcija.*

($\Leftarrow$) : *Neka je $P = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$, sa $a_n \neq 0$, i $Q = b_m t^m + b_{m-1} t^{m-1} + \ldots + b_1 t + b_0$, sa $b_m \neq 0$, i neka je $n \geq m$ (slučaj kada je $n \leq m$ je analogan). Neka je $\psi(P) = \psi(Q)$. Tada za svako $x \in F$ važi $\psi(P)(x) = \psi(Q)(x)$, odakle imamo $\psi(P)(x) - \psi(Q)(x) = 0$, odnosno $(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) - (b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0) = 0$, tj. $a_n x^n + \ldots + a_{m+1} x^{m+1} + (a_m - b_m) x^m + \ldots + (a_1 - b_1) x + (a_0 - b_0) = 0$. Na osnovu prethodne leme sledi da $a_n t^n + \ldots + a_{m+1} t^{m+1} + (a_m - b_m) t^m + \ldots + (a_1 - b_1) t + (a_0 - b_0)$ mora biti nula polinom, odakle sledi $n = m$ (jer smo pretpostavili $a_n \neq 0$) i $a_n = b_n, \ldots, a_0 = b_0$, tj. $P = Q$.*

Polinomske funkcije nad konačnim poljima

Napomena

Iz prethodnih tvrđenja sledi da ako je $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ tačno za sve $x \in F$ i F je beskonačno polje, tada važi $a_n = \ldots = a_0 = 0$. Nad konačnim poljima to nije tačno jer za, npr, $\mathbb{Z}_3$ imamo $x^3 - x = 0$ za sve $x \in \mathbb{Z}_3$. Međutim, ako ograničimo stepene polinoma možemo izvući isti zaključak kao nad beskonačnim poljima.

Teorema

Neka je F polje od m elemenata i $\mathcal{M} \subset F[t]$ takav da $\mathcal{M}$ sadrži nula polinom i sve polinome nad F stepen manjeg od m. Tada za $P \in M$ važi $P = 0$ akko su svi elementi polja F koreni od P.

Dokaz

Ako je $dg(P) < m$ tada P može imati najviše $m - 1$ korena, a pošto je pretpostavka da P ima m korena (svi elementi polja) preostaje da je $P = 0$.

Teorema

Neka su $P, Q \in F[t]$ polinomi stepena manjeg od m i neka je F polje od m elemenata. Tada važi $P = Q$ akko $\psi(P) = \psi(Q)$.

Šta smo danas radili

- Malo istorije: polinomi 5. i većeg stepena ne mogu da se reše pomoću radikala
- Polinomske funkcije: nad beskonačnim i konačnim poljima
- Bezuov stav
- Koreni i faktorizacija