

Test fölötti polinomgyűrűk 2.

Klukovits Lajos

TTIK Bolyai Intézet

2020. október 31.

Polinomfüggvények, polinomok gyökei.

Definíció

Az $f = a_n x^n + \dots + a_1 x + a_0 \in F[x]$ polinom $c \in F$ helyen vett **helyettesítési értéke** az $f(c) = a_n c^n + \dots + a_1 c + a_0 \in F$ elem. Az

$$f: F \rightarrow F, \quad c \mapsto f(c)$$

leképezést az $f \in F[x]$ polinomhoz tartozó **polinomfüggvénynek** nevezzük.

Megjegyzés.

Nagyon fontos a polinom és a polinomfüggvény fogalmának elkülönítése, megkülönböztetése. Erre a következő példák is rámutatnak.

Polinomfüggvények, polinomok gyökei.

Példák.

- Ha F véges test, mondjuk $|F| = q$, akkor az $F \rightarrow F$ leképezések száma q^q , míg az F fölötti polinomok száma végtelen.
- Tekintsük az $f = x^3$ és a $g = x \in \mathbb{Z}_3$ test fölötti polinomokat. Ekkor

$$f: \bar{0} \mapsto \bar{0}^3 = \bar{0}, \quad \bar{1} \mapsto \bar{1}^3 = \bar{1}, \quad \bar{2} \mapsto \bar{2}^3 = \bar{2},$$

azaz ugyanúgy az identikus függvény, mint a g polinomhoz tartozó. Ez azt (is) mutatja, hogy különböző polinomok ugyanazt a polinomfüggvényt határozhatják meg.

Definíció.

Azt mondjuk, hogy az $a \in F$ elem **gyöke (zéróhelye)** az $f \in F[x]$ polinomnak, ha $f(a) = 0$.

Polinomok gyökei.

Bezout tétele

Bármely $f \in F[x]$ és $a \in F$ esetén $f(a) = 0 \iff x - a \mid f$.

Bizonyítás.

Legyen $f \in F[x]$ és $a \in F$ egy tetszőleges.

Maradékos osztást végezve: $f = (x - a)g + b$, ahol $g \in F[x]$, $b \in F$.

Egyszerűen látható, hogy $b = f(a)$, azaz $f = (x - a)g + f(a)$,

amiből azonnal adódik a tétel állítása.

Polinomok gyökei, a Bezout tétel következményei.

1. Következmény.

Tetszőleges $f, g \in F[x]$ esetén a két polinom közös gyökei éppen a legnagyobb közös osztójuk, ln. k. o. (f, g) gyökei.

2. Következmény.

Ha $a_1, \dots, a_k \in F$ páronként különböző elemek, akkor

$$f(a_1) = \dots = f(a_k) = 0 \quad \Leftrightarrow \quad (x - a_1) \dots (x - a_k) | f.$$

Polinomok gyökei.

Definíció.

Az $f \in F[x]$ polinomnak az $\alpha \in F$ **k-szoros gyöke**, ha $(x - \alpha)^k | f$, de $(x - \alpha)^{k+1} \nmid f$. A k az α gyök **multiplicitása**.

Állítás.

Ha az $f \in F[x]$ (nemzéró) polinom fokszáma n , akkor legfeljebb n különböző gyöke van F -ben.

Megjegyzés.

A polinom és a zéróhely fogalmát egységelemes gyűrű fölött is bevezethetjük, de akkor nem érvényes már az előbbi következmény. Például, a $\mathbb{Z}_{12}$ gyűrű fölötti $x^2 - 1$ polinomnak 4 gyöke is van az alapgyűrűben.

Polinomok gyökei.

Állítás.

Ha az $f, g \in F[x]$ polinomok legfeljebb n -edfokúak, és $n + 1$ helyen ugyanaz a helyettesítési értékük, akkor $f = g$.

Állítás.

Ha az F test végtelen, akkor két F fölötti polinom akkor és csak akkor egyenlő, ha a hozzájuk tartozó polinomfüggvények megegyeznek.

Megjegyzés.

Ha az F test véges, akkor könnyen találhatók olyan különböző polinomok F fölött, amelyek ugyanazt a polinomfüggvényt határozzák meg. Például, ha $|F| = p$ prím, akkor ilyenek az x^p és az x polinomok.

Polinomok gyökeinek meghatározása 1.

Ókori előzmények.

- Már az Óbabiloni Birodalom írnokai ismertek olyan eljárásokat, amelyekkel minden olyan másodfokú egyenlet egy pozitív gyökét meg tudták határozni, amelynek volt ilyen gyöke.
- Eljárásuk — amelyet csak verbálisan fogalmaztak meg — lényegében megegyezett azzal, ahogy ma levezetjük a másodfokú egyenletek gyökképletét:
 - ▶ Az „egyenletnek” a másodfokú tagot tartalmazó oldalát teljes négyzetté alakították,
 - ▶ majd négyzetgyököt vontak, amire hatékony algoritmusuk volt.
- Megoldási eljárásuk lényege: a problémát egy elsőfokú egyenlet megoldására vezették vissza.
- Eljárásuk alkalmas $\mathbb{C}$ fölötti másodfokú polinomok összes gyökének meghatározására.

Gyökök meghatározása: harmadfokú egyenletek 1.

Tartaglia a XVI. században.

(1) Az $ax^3 + bx^2 + cx + d = 0$, $a, b, c, d \in \mathbb{C}$ egyenletből $x = y - \frac{b}{3a}$ helyettesítéssel, majd a kezdő együtthatóval való leosztás után

$$y^3 + py + q = 0$$

alakú harmadfokú egyenlethez juthatunk.

(2) Ennek megoldását $y = u + v$ alakban keressük.

(3) Az $(u + v)^3 = (u^3 + v^3) + 3uv(u + v)$ egyenlőségéből

$$(u + v)^3 - 3uv(u + v) - (u^3 + v^3) = 0$$

amiből az $y^3 + py + q = 0$ egyenlettel együtthatónként összehasonlítva:

Gyökök meghatározása: harmadfokú egyenletek 2.

Tartaglia (modernizálva)

(4) az

$$\begin{aligned} 3uv &= -p \\ u^3 + v^3 &= -q \end{aligned}$$

egyenletrendszert kapjuk.

(5) A Viète-képletek alapján u^3, v^3 megoldása a

$$z^2 + qz - \left(\frac{p}{3}\right)^3 = 0$$

másodfokú egyenletnek.

(6) Ebből

$$u^3, v^3 = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

Gyökök meghatározása: harmadfokú egyenletek 3.

Tartaglia (modernizálva)

(7) Köbgyököt vonva u, v -re

$$u, u\varepsilon, u\varepsilon^2, \quad v, v\varepsilon, v\varepsilon^2$$

adódik, ahol ε egy harmadik primitív egységgyök.

(8) Ellenőrizhető, hogy csak az

$$y_1 = u + v, \quad y_2 = u\varepsilon + v\varepsilon^2, \quad y_3 = u\varepsilon^2 + v\varepsilon$$

értékek megoldások, csak ezekre teljesül a (4) pont két egyenlősége.

Gyökök meghatározása: harmadfokú egyenletek 4.

Tartaglia (modernizálva)

(9) Az

$$y = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

összefüggést **Cardano-képletnek** szokás nevezni, mert, DE

Gyökök meghatározása: harmadfokú egyenletek 4.

Példa.

Oldja meg az $x^3 - 6x^2 + 57x - 196 = 0$ egyenletet.

- $x = y + 2$ helyettesítés után az $y^3 + 45y - 98 = 0$ egyenletet kapjuk.
- A Cardano képlettel számolva:

$$u, v = \sqrt[3]{49 \pm \sqrt{49^2 + 15^3}} = \sqrt[3]{49 \pm \sqrt{5776}} \\ = \sqrt[3]{49 \pm 76}$$

- Így $u = 5$, $v = -3$; amiből
- $y_1 = u + v = 2$, $y_2 = u\varepsilon + v\varepsilon^2 = -1 + 4i\sqrt{3}$, $y_3 = u\varepsilon^2 + v\varepsilon = -1 - 4i\sqrt{3}$.
- A megoldás: $x_1 = 4$, $x_{2,3} = 1 \pm 4i\sqrt{3}$.

Gyökök meghatározása: negyedfokú egyenletek 1.

Ferrari (XVI. sz.) eljárása modernizálva.

Tekintsük az $x^4 + ax^3 + bx^2 + cx + d = 0$, $a, b, c, d \in \mathbb{C}$ egyenletet.

A bal oldalt két másodfokú polinom szorzatára bontjuk úgy, hogy előbb két polinom négyzetének különbségaként állítjuk elő:

$$x^4 + ax^3 + bx^2 + cx + d = \left(x^2 + \frac{a}{2}x + \frac{\alpha}{2}\right)^2 \\ - \left(\left(\frac{a^2}{4} + \alpha - b\right)x^2 + \left(\frac{a\alpha}{2} - c\right)x + \left(\frac{\alpha^2}{4} - d\right)\right)$$

Az α paramétert úgy kell meghatározni, hogy a második tag teljes négyzet legyen, azaz

egyik gyöke legyen az $\left(\frac{a\alpha}{2} - c\right)^2 - 4\left(\alpha + \frac{a^2}{4} - b\right)\left(\frac{\alpha^2}{4} - d\right) = 0$ harmadfokú egyenletnek.

Negyedfokú egyenletek 2. Egy példa.

Oldjuk meg az $f = x^4 + 6x^3 + 6x^2 - 8 = 0$ egyenletet.

- 1 $f = (x^2 + 3x + \frac{\alpha}{2})^2 - \left((9 + \alpha - 6)x^2 + 3\alpha x + (8 + \frac{\alpha^2}{4})\right)$,
- 2 $9\alpha^2 - (3 + \alpha)(32 + \alpha^2) = -\alpha^3 + 6\alpha^2 - 32\alpha - 96 = 0$.
- 3 $\alpha = y + 2$ helyettesítés után az $y^3 + 20y + 144 = 0$ egyenlet egy gyökét keressük: $y = -4$, amiből $\alpha = -2$.
- 4 Ezt (1)-be helyettesítve:

$$(x^2 + 3x - 1)^2 - (x^2 - 6x + 9) = (x^2 + 4x - 4)(x^2 + 2x + 2) = 0,$$
- 5 így a gyökök: $x_{1,2} = -2 \pm 2\sqrt{2}$, $x_{3,4} = -1 \pm i$.

Fontos észrevétel.

MIND A HARMAD- MIND A NEGYEDFOKÚ ESETBEN A MEGOLDÁS KULCSA EGY EGYEL ALACSONYABB FOKÚ EGYENLET MEGOLDÁSA VOLT.

Emlékezzünk: a másodfokú egyenleteknél is ugyanez volt a helyzet.

A továbblépés, a fokszám növelésének egyik útja, hogy mindig keressünk olyan eggyel (esetleg többel) alacsonyabb fokú, ún. rezolvens egyenletet, amelynek egy gyökét használva oldhatjuk meg a problémát.

Továbblépés.

Alapvető kérdések.

- 1 Egészen a XVIII. század utolsó évtizedeig minden matematikus nyilvánvalónak tekintette, hogy az egyenletek megoldhatók, azaz
- 2 minden komplex számtest fölötti polinomnak van komplex zéróhelye.
- 3 E hiedelem annyira erős volt, hogy nem is foglalkoztak a bizonyításával.
- 4 Sőt az is erős hiedelem volt, hogy a zéróhelyek/gyökök előállíthatók (ún. algebrai eszközökkel) a polinom/egyenlet együtthatóiból.

A (klasszikus) algebra alaptétele. GAUSS 1799.

Theorem

Minden legalább elsőfokú komplex együtthatós polinomnak van komplex zéróhelye,

Továbblépés.

Válasz kísérletek.

Gauss tétele válasz az (1) és (2)-beli kérdésekre, de a (4)-ben említett hiedelem a XVIII-XIX. század fordulóján már ingani kezdett.

A több évszázados sikertelen kísérletek után a XIX. század elején többen is megtalálni vélték az ötödfokú egyenletek „gyökképletét”, de hamarosan rájöttek, hogy bizonyításaik hibásak, sőt inkább az látszott igazolódni, hogy nincs ilyen képlet.

Pontos fogalmak/kérdésfeltevések hiányában a „bizonyítások” is hibásnak bizonyultak.

Nils Henrik ABEL, 1826.

Az ötöd- és magasabbfokú egyenletekhez nem létezik gyökképlet (általános megoldási eljárás).

Interpoláció.

Lagrange interpolációs tétele.

Tetszőleges, páronként különböző $c_1, \dots, c_{n+1}$ és tetszőleges $d_1, \dots, d_{n+1}$ (nem feltétlenül különböző) F -beli elemekhez pontosan egy olyan $f \in F[x]$ legfőljebb n -edfokú polinom létezik, amelyre $f(c_i) = d_i$ minden $i \in \{1, 2, \dots, n+1\}$ -re.

Definíció.

Az előbbi f az ún. **Lagrange-féle interpolációs polinom**.

Megjegyzés.

Előfordulhat, hogy az $n+1$ pontra illeszkedő Lagrange-polinom fokszáma kisebbnek adódik n -nél. Pontosan n -edfokú polinom létezése nem garantálható. Ha azonban semmit sem kötünk ki a fokszámra, akkor elvesz az unicitás. Ugyanis tetszőleges $g \in F[x]$ polinomra az $f + (x - c_1) \dots (x - c_{n+1})g$ polinomra is teljesül a helyettesítési értékre vonatkozó föltétel.

Irreducibilis faktorizáció.

Definíció.

A $p \in F[x]$ polinom **irreducibilis** (az $F[x]$ **polinomgyűrűben**, ill. **irreducibilis F fölött**), ha legalább elsőfokú és csak triviális módon bontható föl F fölötti polinomok szorzatára, azaz ha valamely $f, g \in F[x]$ polinomokra $p = fg$, akkor $f \sim p$, vagy $g \sim p$. (Ekkor nyilván $g \sim 1$, vagy $f \sim 1$.) Formálisan: $\forall f, g \in F[x]: p = fg \Rightarrow (f \sim p \text{ vagy } g \sim p)$.

Állítás.

Egy legalább elsőfokú $p \in F[x]$ polinom akkor és csak akkor irreducibilis F fölött, ha nem bontható föl deg p -nél alacsonyabb fokú, $F[x]$ -beli polinomok szorzatára.

Megjegyzés.

Lényeges, hogy mely test fölött tekintjük a polinomot: az $x^2 - 2$ polinom $\mathbb{Q}$ fölött irreducibilis, de pl. $\mathbb{R}$ fölött már nem.

Irreducibilis faktorizáció.

Definíció.

A $p \in F[x]$ polinom **prím**, másszóval **prímtulajdonságú**, ha legalább elsőfokú, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat valamelyik tényezőjének.

Theorem

Test fölötti polinomgyűrűkben az irreducibilitás és a prímtulajdonság ekvivalens, azaz egy test fölötti polinom pontosan akkor prím, ha irreducibilis.

Irreducibilis faktorizáció.

Bizonyítás.

- (1) Legyen $f \in F[x]$ irreducibilis és $f|gh$, $g, h \in F[x]$.
- (2) Tegyük föl, hogy $f \nmid g$. Ekkor $\text{In. k. o.}(f, g) \sim 1$.
- (3) Léteznek olyan $u, v \in F[x]$ polinomok, hogy $fu + gv = 1$.
- (4) h -val szorozva ezen egyenlőséget kapjuk, hogy $f|h$.
- (5) Legyen $f \in F[x]$ prím és $f = gh$, $g, h \in F[x]$.
- (6) Ha $f|g$, akkor $g = fu$, $u \in F[x]$, ekkor $f = (fu)h$,
- (7) ebből $1 = uh$, azaz u egység.

□

Irreducibilis faktorizáció.

Theorem

Minden legalább elsőfokú $f \in F[x]$ polinom fölbontható irreducibilis polinomok szorzatára. A fölbonthatóság a tényezők sorrendjétől, és asszociáltságtól eltekintve egyértelműen meghatározott.

Bizonyítás.

- 1 Ha f irreducibilis, készen vagyunk. Ha nem,
- 2 Léteznek olyan $g, h \in F[x]$ nemkonstans polinomok, hogy $f = gh$, és $\deg g, \deg h < \deg f$.
- 3 Ha mindkettő irreducibilis, készen vagyunk. Ha valamelyik nem, arra megismételjük az előbbi eljárást.
- 4 A fokszámra kirótt feltétel miatt ezen eljárás véges, az utolsó lépésben már mindegyik tényező irreducibilis.
- 5 Az egyértelműség abból adódik, hogy az irreducibilis polinomok prímtulajdonságúak.

Irreducibilis faktorizáció.

Tétel.

Ha a legalább másodfokú $f \in F[x]$ polinom irreducibilis, akkor nincs gyöke F -ben.

Megjegyzés.

Az előbbi tétel megfordítása nem igaz. Egy ellenpélda az $x^4 + 1 \in \mathbb{R}[x]$ polinom.

Tétel.

Legyen $f \in F[x]$ és $2 \leq \deg f \leq 3$. F pontosan akkor irreducibilis, ha nincs gyöke.

Tétel.

Az $F[x]/(f)$ maradékosztály-gyűrű pontosan akkor test, ha az f polinom irreducibilis F fölött.