Algebra és számelmélet előadás

Waldhauser Tamás
2016. október 13.

Ötödik házi feladat az előadásra

Az alábbi linken megtalálható a test feletti polinomok maradékos osztásáról szóló tétel *kissé hiányos* bizonyítása:

`https://www.overleaf.com/articles/eahf5/nfhdcbrdqvgg`

Töltse ki a hiányzó részeket úgy, hogy a tétel (matematikailag és nyelvileg) helyes bizonyítását kapja.

- beküldendő emailben: `twaldha@math.u-szeged.hu`
- pdf fájl legyen (lehet szkennelt is)
- fájlnév: `EHA-eahf5.pdf` (például `WATHAAS-eahf5.pdf`)
- határidő: október 26, reggel 8 óra

A gyökök száma

3.23. Következmény.

Ha az $0 \neq f \in T[x]$ polinom fokszáma n, akkor legfeljebb n különböző gyöke van a T testben.

Bizonyítás.

Legyenek $\alpha_1, \ldots, \alpha_k \in T$ az f polinom összes különböző gyökei. Ekkor

$$(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \implies k \leq \deg f = n. \qquad \square$$

Megjegyzés.

Ha nem *test* feletti polinomokat tekintünk, akkor a gyökök száma meghaladhatja a fokszámot! Például az $x^2 - \overline{1} \in \mathbb{Z}_{12}[x]$ polinomnak négy gyöke is van!

Polinom vs. polinomfüggvény

3.24. Következmény.

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

Bizonyítás.

Ha a legfelljebb n-edfokú $h := f - g$ polinomnak van $n+1$ gyöke, akkor $h = 0$.

□

3.25. Következmény.

Ha a T test végtelen, akkor két T feletti polinom akkor és csak akkor egyenlő, ha a hozzájuk tartozó polinomfüggvények megegyeznek.

3.26. Megjegyzés.

Ha a T test véges, akkor találhatók különböző T feletti polinomok, amelyekhez ugyanaz a polinomfüggvény tartozik (keressünk végtelen sok ilyen példát!). Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Lagrange-interpoláció

3.27. Tétel (Lagrange-interpoláció).

Tetszőleges $c_1, \ldots, c_{n+1}$ páronként különböző és $d_1, \ldots, d_{n+1}$ (nem feltétlenül különböző) T-beli elemekhez létezik pontosan egy $f \in T[x]$ legfeljebb n-edfokú polinom, amelyre $f(c_i) = d_i \ \ (i = 1, \ldots, n+1)$ teljesül.

3.28. Definíció.

Az előző tételbeli f polinom neve *Lagrange-féle interpolációs polinom*.

3.29. Megjegyzés.

Előfordulhat, hogy az $n+1$ pontra illesztett Lagrange-féle interpolációs polinom foka kisebb, mint n. Pontosan n-edfokú polinom létezését nem lehet garantálni. Ha nem kötünk ki semmit a fokszámra, akkor elveszítjük az unicitást: bármely $g \in T[x]$ polinomra $f + (x - c_1) \cdots (x - c_{n+1}) \cdot g$ is megfelelő. Nem nehéz meggondolni (tegyük meg!), hogy minden olyan polinom, amely a c_i helyeken a d_i értékeket veszi fel, előáll ilyen alakban.

Lagrange-interpoláció

Példa.

Határozza meg azt a legalacsonyabb fokszámú $f \in \mathbb{R}[x]$ polinomot, amelyre

$$f(0) = 1,\ f(1) = 2,\ f(2) = 4,\ f(3) = 8.$$

$$\begin{aligned} \Phi_1 &= (x-1)(x-2)(x-3) & \Phi_1(0) &= -6 \\ \Phi_2 &= x(x-2)(x-3) & \Phi_2(1) &= 2 \\ \Phi_3 &= x(x-1)(x-3) & \Phi_3(2) &= -2 \\ \Phi_4 &= x(x-1)(x-2) & \Phi_4(3) &= 6 \end{aligned}$$

$$f = 1 \cdot \frac{\Phi_1}{-6} + 2 \cdot \frac{\Phi_2}{2} + 4 \cdot \frac{\Phi_3}{-2} + 8 \cdot \frac{\Phi_4}{6} = \frac{1}{6}x^3 + \frac{5}{6}x + 1 = \binom{x}{0} + \binom{x}{1} + \binom{x}{2} + \binom{x}{3}$$

Házi feladat a gyakorlatra

16. feladat. Határozza meg azt a legalacsonyabb fokszámú $f \in \mathbb{C}[x]$ polinomot, amely a megadott helyeken a megadott értékeket veszi fel.

(a) $f(0) = 1,\ f(1) = 2,\ f(2) = 4,\ f(3) = 8$

$f = \frac{1}{6}x^3 + \frac{5}{6}x + 1$

(b) $f(-1) = 6,\ f(0) = 5,\ f(1) = 0,\ f(2) = 3,\ f(3) = 2$

$f = -x^4 + 4x^3 - x^2 - 7x + 5$

(c) $f(1) = 2,\ f(i) = i$

(d) $f(1) = 2,\ f(2) = 1,\ f(3) = 4,\ f(4) = 3$

(e) $f(1) = 0,\ f(2) = 1,\ f(3) = 3,\ f(4) = 6$

Irreducibilis polinomok, véges testek

Évariste Galois

(1811, Bourg-la-Reine – 1832, Párizs)

Irreducibilitás

3.30. Definíció.

A $p \in T[x]$ polinom *irreducibilis*, ha legalább elsőfokú, és csak úgy bontható két polinom szorzatára, hogy az egyik tényező asszociált p-hez. (Ekkor a másik tényező szükségképpen asszociált 1-hez; ilyenkor *triviális faktorizációról* beszélünk.)
Formálisan:

$$\forall f, g \in T[x] : p = fg \implies (p \sim f \text{ vagy } p \sim g).$$

3.31. Állítás.

Egy legalább elsőfokú $p \in T[x]$ polinom akkor és csak akkor irreducibilis, ha p nem bontható $\deg p$-nél kisebb fokszámú polinomok szorzatára.

Bizonyítás.

- triviális felbontás: $p = f \cdot g$, ahol $\deg f = 0, \deg g = \deg p$ (vagy fordítva)
- nemtriviális felbontás: $p = f \cdot g$, ahol $1 \leq \deg f, \deg g < \deg p$

□

Egyértelmű irreducibilis faktorizáció

3.32. Definíció.

A $p \in T[x]$ polinom *prím*, ha legalább elsőfokú, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall f, g \in T[x] : p \mid fg \implies (p \mid f \text{ vagy } p \mid g).$$

3.33. Tétel.

Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.

3.34. Tétel.

Minden legalább elsőfokú polinom felbontható irreducibilis polinomok szorzatára.

Ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelműen meghatározott, azaz ha $p_1 \cdot \ldots \cdot p_n$ és $q_1 \cdot \ldots \cdot q_m$ ugyanazon polinom két irreducibilis faktorizációja, akkor $n = m$, és létezik olyan $\pi \in S_n$ permutáció, hogy minden $i = 1, \ldots, n$ esetén

$$p_i \sim q_{\pi(i)}.$$

Irreducibilitás vs. gyökök

3.35. Állítás.

Az elsőfokú polinomok bármely test felett irreducibilisek.

Bizonyítás.

Ha $f = g \cdot h$, akkor $\deg g + \deg h = 1$, és így

$$\deg g = 1, \deg h = 0 \quad \text{vagy} \quad \deg g = 0, \deg h = 1.$$

Mindkét esetben triviális a felbontás. □

3.36. Tétel.

Ha $f \in T[x]$ irreducibilis és $\deg f \geq 2$, akkor f-nek nincs gyöke.

Bizonyítás.

Ha α gyöke f-nek, akkor $f = (x - \alpha)(\cdots)$ nemtriviális felbontás. □

Irreducibilitás vs. gyökök

3.37. Tétel.

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

Bizonyítás.

Ha $f = g \cdot h$, akkor $\deg g + \deg h \in \{2, 3\}$, így a nemtriviális felbontásokra a következő lehetőségek vannak:

$\deg f$	$\deg g$	$\deg h$
2	1	1
3	2	1
3	1	2

Tehát f akkor és csak akkor nem irreducibilis, ha van elsőfokú osztója. Egy elsőfokú polinom asszociáltság erejéig mindig $x - \alpha$ alakban írható* , ez pedig akkor és csak akkor osztja f-et, ha α gyöke f-nek. □

*$ax + b = a\left(x + \frac{b}{a}\right) \sim x + \frac{b}{a} = x - \left(-\frac{b}{a}\right) = x - \alpha$

Irreducibilitás vs. gyökök

Összefoglalva:

Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

implikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz: azok mindig irreducibilisek és mindig van gyökük!

A

$$\text{nincs gyöke} \implies \text{irreducibilis}$$

implikáció igaz a másod- és harmadfokú polinomokra, de magasabbfokúakra nem!

Példa.

Az $f = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ polinomnak nincs valós gyöke, mégsem irreducibilis $\mathbb{R}$ felett:

$$f = (x^2 + 1)(x^2 + 1).$$

Irreducibilitás vs. gyökök

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM NEM NEM NEM NEM NEM NEM

KÖVETKEZIK

AZ IRREDUCIBILITÁS!!!

Irreducibilis faktorizáció

Példa.

Bontsa irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = x^6 + 3x^4 - x^3 + 2x^2 + x - 1 \in \mathbb{Z}_5[x].$$

Mivel az alaptestnek csak öt eleme van, egyenként kipróbálhatjuk, hogy gyöke-e valamelyik az f polinomnak.

Amelyik igen, annál a Horner-módszerrel megállapítjuk a multiplicitást, és leválasztjuk a gyöktényezőket:

$$f = (x-1)^2 (x-3)(x-4)(x^2 + 4x + 2).$$

Az $x^2 + 4x + 2$ polinomnak nincs gyöke (ha lenne, megtaláltuk volna), és csak másodfokú, ezért irreducibilis.

(Ha negyed- vagy magasabb fokú polinom marad a gyöktényezők kiemelése után, akkor valami trükkre van szükség . . .)

Házi feladat a gyakorlatra

17. feladat. Bontsa irreducibilis tényezők szorzatára a polinomokat a megadott polinomgyűrűkben.

(a) $x^6 + \overline{3}x^4 - x^3 + \overline{2}x^2 + x - \overline{1} \in \mathbb{Z}_5[x]$

$(x - \overline{1})^2 (x - \overline{3}) (x - \overline{4}) (x^2 + \overline{4}x + \overline{2})$

(b) $x^5 + x^4 + \overline{2}x^3 + x^2 + \overline{1} \in \mathbb{Z}_3[x]$

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

(c) $x^5 + x^4 + \overline{2}x^3 + \overline{2}x + \overline{1} \in \mathbb{Z}_3[x]$

(d) $x^5 + x^4 + \overline{2}x^3 + \overline{1} \in \mathbb{Z}_5[x]$

(e) $x^5 + x^3 + \overline{4}x^2 + \overline{4} \in \mathbb{Z}_5[x]$

Polinomgyűrű faktorteste

3.38. Tétel.

A $T[x]/(m)$ maradékosztály-gyűrű akkor és csak akkor test, ha m irreducibilis T felett.

Bizonyítás.

Tudjuk, hogy

1. $T[x]/(m)$ kommutatív egységelemes gyűrű (3.14. Áll.);
2. $T[x]/(m)$ egységcsoportja: $\left\{\overline{f} : f \perp m\right\}$ (3.15. Tétel);
3. tehát $T[x]/(m)$ akkor és csak akkor test, ha legalább kételemű, és

$$(*) \qquad \forall f \in T[x] : \; m \nmid f \implies f \perp m \qquad \text{(2.4. Def.)}.$$

- Ha $m \in T \setminus \{0\}$, akkor (és csak akkor) $T[x]/(m)$ egyelemű, tehát nem test.
- Ha $m = 0$, akkor $(*)$-ra $f = x$ egy ellenpélda. (Ekkor $T[x]/(m) \cong T[x]$.)
- Ha $m = f \cdot g$ egy nemtriviális felbontás, akkor $(*)$-ra f egy ellenpélda.
- Ha m irreducibilis, akkor $(*)$ teljesül, mert $\operatorname{lnko}(f, m)$ csak 1 vagy m lehet.

□

Házi feladat a gyakorlatra

18. feladat. Döntse el, hogy testek-e a megadott faktorgyűrűk, és határozza meg elemeik számát.

(a) $\mathbb{Z}_2[x] / (x^3 + x^2 + 1)$

8-elemű, test

(b) $\mathbb{Z}_5[x] / (x^2 + 1)$

25-elemű, nem test

(c) $\mathbb{Z}_5[x] / (x^3 + 2)$

(d) $\mathbb{Z}_3[x] / (x^2 + 1)$

(e) $\mathbb{Z}_3[x] / (x^3 + x^2 + 1)$

Polinomgyűrű faktorteste

3.39. Tétel.

Legyen T test, $m \in T[x]$ irreducibilis polinom, és jelölje n az m polinom fokszámát. Ekkor a $K = T[x]/(m)$ faktorgyűrű olyan test, amelyben az m polinomnak van gyöke. A K test minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban. Ha $T = \mathbb{Z}_p$, akkor $|K| = p^n$.

Bizonyítás.

A maradékos osztás tétele (3.5. Tétel) szerint

$$\forall f \in T[x] \ \exists! r \in T[x] : \ f \equiv r \pmod{m} \text{ és } \deg r \leq n-1.$$

Ezért $T[x]/(m)$ minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban.
Ha $T = \mathbb{Z}_p$, akkor p választási lehetőségünk van minden a_i-re ezért összesen p^n-féleképp tudjuk az $a_{n-1}, \ldots, a_1, a_0$ (n db) együtthatókat megválasztani.

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T). \end{aligned}$$

Hasonló számolás mutatja, hogy

$$m(\alpha) = m(\overline{x}) = \overline{m(x)} = \overline{0},$$

hiszen $m \equiv 0 \pmod{m}$. Tehát $\alpha \in K$ valóban gyöke m-nek. □

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Ha az $m = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in T[x]$ irreducibilis főpolinomnak akarunk „gyököt csinálni”, akkor a $K = T[x] / (m)$ testet kell elkészítenünk.

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T).$$

Az α szimbólumról csak annyit kell tudni, hogy $m(\alpha) = 0$, azaz $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$. Tehát a számolási szabály:

$$\alpha^n = -b_{n-1}\alpha^{n-1} - \cdots - b_1\alpha - b_0.$$

(És ha m nem irreducibilis?)

Egyszerű algebrai bővítés

3.40. Következmény.

Tetszőleges T test és $f \in T[x]$ irreducibilis polinom esetén létezik olyan K test, amelyre

1. K *bővítése* T-nek, azaz $K \supseteq T$;
2. létezik olyan $\alpha \in K$ elem, amely gyöke f-nek;
3. K minden eleme egyértelműen előáll $a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$ $(a_{n-1}, \ldots, a_0 \in T)$ alakban, ahol $n = \deg f$.

Bizonyítás.

Legyen $K = T[x]/(f)$, és alkalmazzuk az előző tételt. □

3.41. Definíció.

Azt mondjuk, hogy a K test T-ből az α elem *adjungálásával* keletkezik (jelölés: $K = T(\alpha)$), és az ilyen módon előálló testeket T *egyszerű algebrai bővítéseinek* nevezzük.

A komplex számtest újratöltve

3.42. Megjegyzés.

Ha a K testet a $T = \mathbb{R}$ és $f = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

Most $n = 2$, tehát

$$K = \{\overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R}\}.$$

Vegyük észre, hogy $\overline{x}^2 = \overline{-1}$, hiszen $x^2 \equiv -1 \pmod{x^2+1}$.

Írjunk $\overline{x}$ helyett i betűt, és hagyjuk el a vonásokat a konstansokról.

Ekkor K egy tipikus eleme:

$$\overline{a_0 + a_1 x} = \overline{a_0} + \overline{a_1} \cdot \overline{x} = a_0 + a_1 \cdot i.$$

Tehát K elemei $a_0 + a_1 \cdot i$ $(a_0, a_1 \in \mathbb{R})$ alakúak, és az i szimbólumra vonatkozó (egyetlen) számolási szabály: $i^2 = -1$.

Tehát $\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[x] / (x^2 + 1)$, és ezt tekinthetnénk akár a komplex számok definíciójának is.