Klasszikus algebra előadás

Waldhauser Tamás
2014. március 24.

Irreducibilitás

3.33. 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:

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

3.34. 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 $1 \leq \deg f, \deg g < \deg p$

□

Egyertelmű irreducibilis faktorizáció

3.35. Definíció.

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

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

3.36. Tétel.

Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.

3.37. 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

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

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 (3.15. Állítás);
2. $T[x]/(m)$ egységcsoportja: $\{\overline{f} : \operatorname{lnko}(f, m) \sim 1\}$ (3.16. Tétel);
3. tehát $T[x]/(m)$ akkor és csak akkor test, ha legalább kételemű, és

   $(*)$ $\quad \forall f \in T[x] : \ \operatorname{lnko}(f, m) \nsim 1 \iff m \mid f$ (2.19. Megjegyzés).

- 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 $T[x]/(m) \cong T$.)
- 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.

□

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?)

A komplex számtest újratöltve

3.40. 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: $i^2 = -1$.

Egy véges test

Példa.

Számoljunk a $\mathbb{Z}_2[x] / (x^3+x+1)$ testben! Ennek  8 eleme van:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}.$$

$$\overline{x+1}+\overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1}\cdot\overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3+\alpha+1=0, \quad \text{azaz} \quad \alpha^3=\alpha+1.$$

$$(\alpha+1)+(\alpha^2+\alpha) = \alpha^2+2\alpha+1 = \alpha^2+1 \qquad \text{(s.v.)}$$

$$(\alpha+1)\cdot(\alpha^2+\alpha) = \alpha^3+2\alpha^2+\alpha = \alpha^3+\alpha = (\alpha+1)+\alpha = 1 \qquad \text{(sz.sz.)}$$

A nyolcelemű test művelettáblázatai

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Egy végtelen test

Példa.

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2+bx+c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\begin{aligned}
\overline{2-x}^{-1} = \overline{u} &\iff \overline{2-x} \cdot \overline{u} = \overline{1} \\
&\iff (2-x)\,u \equiv 1 \pmod{x^3-7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2-x)\,u = 1 + \left(x^3-7\right) v \\
&\iff u \equiv x^2+2x+4 \pmod{x^3-7} \\
&\iff \overline{u} = \overline{x^2+2x+4}
\end{aligned}$$

Tehát $\overline{2-x}^{-1} = \overline{x^2+2x+4}$.

Egy végtelen test

Példa (folyt.).

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$! (Vagy $\alpha = \sqrt[3]{7}\,\mathrm{cis}\,\frac{\pm 2\pi}{3}$.) Tehát K tekinthető számtestnek is:

$$K = \left\{ a\sqrt[3]{49} + b\sqrt[3]{7} + c \colon a, b, c \in \mathbb{Q} \right\}.$$

Az előbb kiszámoltuk, hogy $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$, ami azt jelenti, hogy $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$, azaz

$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$

Ezzel a módszerrel (lényegében az euklideszi algoritmussal) lehet bonyolult nevezőket gyöktelenníteni.

Véges testek

3.41. Tétel*.

Akkor és csak akkor létezik q-elemű test, ha q prímhatvány.

Bizonyítás helyett.

Bármely p prímszám és n pozitív egész szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett (messze nem triviális!).

Ha $f \in \mathbb{Z}_p[x]$ egy ilyen polinom, akkor $T[x] / (f)$ egy p^n-elemű test.

Ha K egy q-elemű test, akkor tartalmaz prím elemszámú résztestet (közel sem triviális!).

Ha T egy p-elemű részteste K-nak, akkor K vektorteret alkot T felett.

Ha ez a vektortér n-dimenziós, akkor $K \cong T^n$, ezért $|K| = p^n$. □

A q-elemű testet (mely izomorfia erejéig egyértelműen meghatározott), Galois tiszteletére $\mathrm{GF}(q)$ jelöli (Galois Field).

Véges testek

Példa.

- kételemű test:  $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test:  $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test:  $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / (x^2 + x + 1)$
- ötelemű test:  $\mathrm{GF}(5) \cong \mathbb{Z}_5$
- hatelemű test:  nincs!
- hételemű test:  $\mathrm{GF}(7) \cong \mathbb{Z}_7$
- nyolcelemű test:  $\mathrm{GF}(8) \cong \mathbb{Z}_2[x] / (x^3 + x + 1)$
- kilencelemű test:  $\mathrm{GF}(9) \cong \mathbb{Z}_3[x] / (x^2 + 1) = \{a + bi : a, b \in \mathbb{Z}_3\}$
- tízelemű test:  nincs!
- ...

Irreducibilitás vs. gyökök

3.42. 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. □

3.43. 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

3.44. 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!!!

Egy irreducibilis faktorizáció

Példa.

Bontsuk 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 . . .)

Irreducibilitás különböző testek felett

Példa.
Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik:  $x^2 + 1 = (x + i)(x - i)$.

Példa.
Az $f = x^2 - 2 \in \mathbb{Q}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{R}[x]$-ben már felbomlik:  $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.
(És persze $\mathbb{C}[x]$-ben is felbomlik.)

Általában, minél nagyobb az alaptest, annál „több esélye" van egy polinomnak felbomlani.

Ha T részteste K-nak és $f \in T[x]$, akkor

$$f \text{ irreducibilis } K \text{ felett } \begin{array}{c} \Rightarrow \\ \not\Leftarrow \end{array} \quad f \text{ irreducibilis } T \text{ felett.}$$

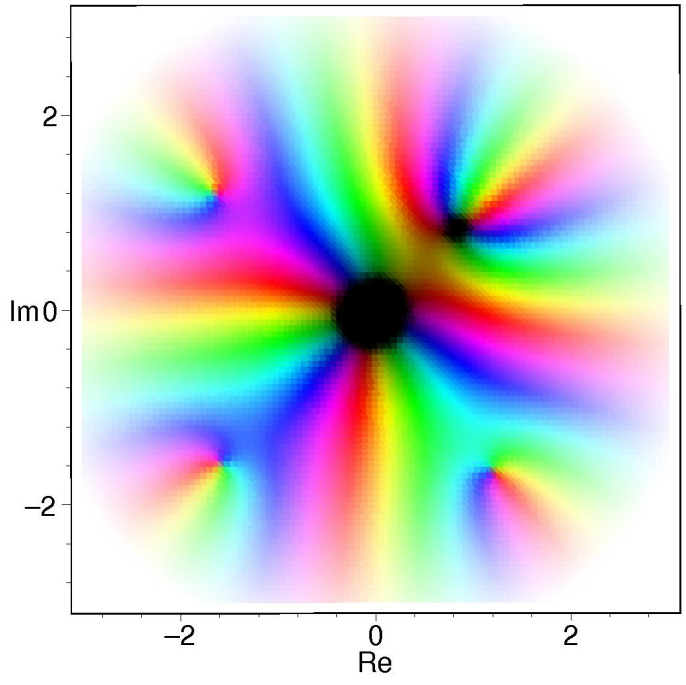
Az algebra alaptétele

3.45. Tétel* (az algebra alaptétele).

Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

Első nem-bizonyítás.

Vizsgáljuk meg egy tetszőleges $f \in \mathbb{C}[x]$ legalább elsőfokú polinom „színképét”:



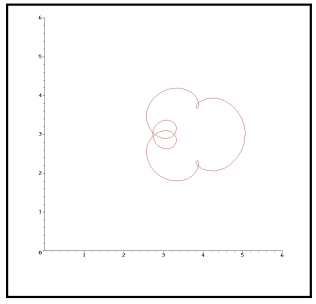
A színképnek van legsötétebb pontja, és ez a pont csak fekete lehet.

Az algebra alaptétele

Második nem-bizonyítás.

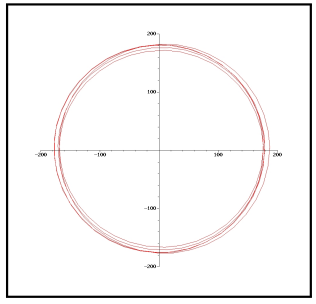
Legyen $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$. Vizsgáljuk meg egy origó középpontú, r sugarú körvonal f melletti képét. Ez egy zárt görbe lesz, amely

- nagyon kicsi r esetén  a_0 körül kunkorodik:



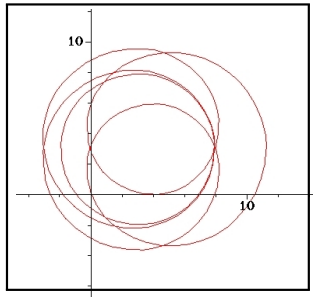
,

- nagyon nagy r esetén  n-szer megkerüli az origót:



.

A kettő közötti folytonos átmenet során a görbe átmegy az origón:



.

Irreducibilis polinomok a komplex számtest felett

3.46. Következmény.

A komplex számok teste felett pontosan az elsőfokú polinomok irreducibilisek.

Bizonyítás.

Tudjuk, hogy az elsőfokúak bármely test felett irreducibilisek.

Ha $f \in \mathbb{C}[x]$ legalább másodfokú, akkor az algebra alaptétele szerint van valódi (pl. elsőfokú) osztója. 

□

Irreducibilis faktorizáció a komplex számtest felett

3.47. Következmény.

Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik.

Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, *akkor* f*-nek multiplicitással számolva pontosan* n *gyöke van.*

Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (*mindegyiket annyiszor feltüntetve, amennyi a multiplicitása*), *akkor*

$$f = a_n (x - \alpha_1) \cdots (x - \alpha_n).$$

Ezt nevezzük a polinom gyöktényezős felbontásának.

Bizonyítás.

Mivel $\mathbb{C}$ test, minden $\mathbb{C}$ feletti legalább elsőfokú polinom irreducibilisek, azaz elsőfokúak szorzatára bomlik. Ezek az elsőfokúak asszociáltság erejéig $x - \alpha$ alakúak. Tehát $f \in \mathbb{C}[x]$ irreducibilis faktorizációja így fest:

$$f \sim (x - \alpha_1) \cdots (x - \alpha_n).$$

Világos, hogy ekkor f gyökei éppen az $\alpha_1, \ldots, \alpha_n$ komplex számok. □

Oszthatóság vs. gyökök

3.48. Következmény.

Bármely $f, g \in \mathbb{C}[x]$ esetén $f \mid g$ akkor és csak akkor teljesül, ha f minden gyöke egyúttal gyöke g-nek is, mégpedig legalább akkora multiplicitással, mint f-nek.

Bizonyítás.

Az f polinom gyökei „egy az egybe” megfelelnek f prímosztóinak, továbbá az α gyök multiplicitása éppen az $x - \alpha$ prímtényező kitevője f prímfelbontásában.

A prímfelbontásból pedig ugyanúgy lehet az oszthatóságot kiolvasni, mint az egész számok körében. □

Valós polinom komplex gyökei

3.49. Tétel.

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \forall z \in \mathbb{C} : f(z) = 0 \implies f(\bar{z}) = 0.$$

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$\begin{aligned} f(\overline{z}) &= a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0 \\ &= \overline{a_n} \cdot \overline{z}^n + \cdots + \overline{a_1} \cdot \overline{z} + \overline{a_0} \\ &= \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} \\ &= \overline{a_n z^n + \cdots + a_1 z + a_0} \\ &= \overline{f(z)} \end{aligned}$$

Tehát $f(z) = 0 \implies f(\overline{z}) = \overline{f(z)} = \overline{0} = 0$. □

Irreducibilis polinomok a valós számtest felett

3.50. Következmény.

Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste felett, ha elsőfokú, vagy olyan másodfokú polinom, melynek nincs valós gyöke. Tehát az $\mathbb{R}$ feletti irreducibilis polinomok a következők:

- $ax + b \ \ (a, b \in \mathbb{R}, a \neq 0)$;
- $ax^2 + bx + c \ \ \left(a, b, c \in \mathbb{R}, a \neq 0, b^2 - 4ac < 0\right)$.

Bizonyítás.

Tudjuk, hogy a legfeljebb másodfokú polinomok között pontosan a fentiek az irreducibilisek. Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett.
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek, és $\overline{\alpha} \neq \alpha$  mert $\alpha \notin \mathbb{R}$. Ezért az $(x - \alpha)(x - \overline{\alpha}) \mid f$ oszthatóság teljesül $\mathbb{C}[x]$-ben. Node

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - 2\operatorname{Re}\alpha \cdot x + |\alpha|^2 \in \mathbb{R}[x],$$

  így f-nek $(x - \alpha)(x - \overline{\alpha})$ valódi osztója $\mathbb{R}[x]$-ben (miért?).  □

Irreducibilis faktorizáció a valós számtest felett

Példa.

Határozzuk meg az $f = x^6 - 27$ polinom irreducibilis felbontását $\mathbb{R}$ felett.

A polinom komplex gyökei:  $\sqrt{3}$, $-\sqrt{3}$, α, $\overline{\alpha}$, β, $\overline{\beta}$, ahol

$$\alpha = \sqrt{3} \cdot \left(\frac{1}{2} + \frac{\sqrt{3}}{2} i \right) = \frac{\sqrt{3}}{2} + \frac{3}{2} i, \qquad \beta = \sqrt{3} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i \right) = -\frac{\sqrt{3}}{2} + \frac{3}{2} i$$

A $\mathbb{C}$ feletti felbontás (azaz a gyöktényezős alak):

$$f = (x - \sqrt{3})(x + \sqrt{3})\,(x - \alpha)\,(x - \overline{\alpha})\,(x - \beta)\,\left(x - \overline{\beta}\right).$$

Az $\mathbb{R}$ feletti felbontás:

$$\begin{aligned} f = &\ (x - \sqrt{3})(x + \sqrt{3})\left(x^2 - 2\,\mathrm{Re}\,\alpha \cdot x + |\alpha|^2\right)\left(x^2 - 2\,\mathrm{Re}\,\beta \cdot x + |\beta|^2\right) \\ = &\ (x - \sqrt{3})(x + \sqrt{3})\left(x^2 - \sqrt{3}x + 3\right)\left(x^2 + \sqrt{3}x + 3\right). \end{aligned}$$

A $\mathbb{Q}$ feletti felbontás:

$$f = (x^2 - 3)(x^4 + 3x^2 + 9).$$