Algebra és számelmélet előadás

Waldhauser Tamás
2016. október 20.

Egy véges test

Példa.

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

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

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

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

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	$\alpha+1$

Házi feladat a gyakorlatra

19. feladat. Számítsa ki a véges testek megadott elemeit.

(a) $\mathbb{Z}_2[x] / (x^3 + x + 1)$-ben $\quad \overline{x}^{-1} = ?, \quad \overline{x^2}^{-1} = ?$

$\overline{x}^{-1} = \overline{x^2 + 1}, \quad \overline{x^2}^{-1} = \overline{x^2 + x + 1}$

(b) $\mathbb{Z}_3[x] / (x^3 - x + 1)$-ben $\quad \overline{2x^2 + 1}^{-1} = ?, \quad \overline{x} / \overline{x + 1} = ?$

$\overline{2x^2 + 1}^{-1} = \overline{x}, \quad \overline{x} / \overline{x + 1} = \overline{x^2 + 2x + 1}$

(c) $\mathbb{Z}_5[x] / (x^3 + x + 2)$-ben $\quad \overline{x^2 + 1}^{-1} = ?, \quad \overline{4x + 3} / \overline{x^2} = ?$

(d) $\mathbb{Z}_7[x] / (x^3 + x + 1)$-ben $\quad \overline{2x}^{-1} = ?, \quad \overline{x} / \overline{2x + 2} = ?$

(e) $\mathbb{Z}_5[x] / (x^3 + x^2 + 2)$-ben $\quad \overline{x + 1}^{-1} = ?, \quad \overline{x^2} / \overline{3x + 4} = ?$

Egy végtelen faktortest

Példa.

Határozza meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ 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.

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

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

Gyöktelenítés

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

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

Irreducibilis polinomok $\mathbb{C}$ és $\mathbb{R}$ felett, gyöktényezős alak

François Viète

(1540, Fontenay-le-Comte – 1603, Párizs)

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

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

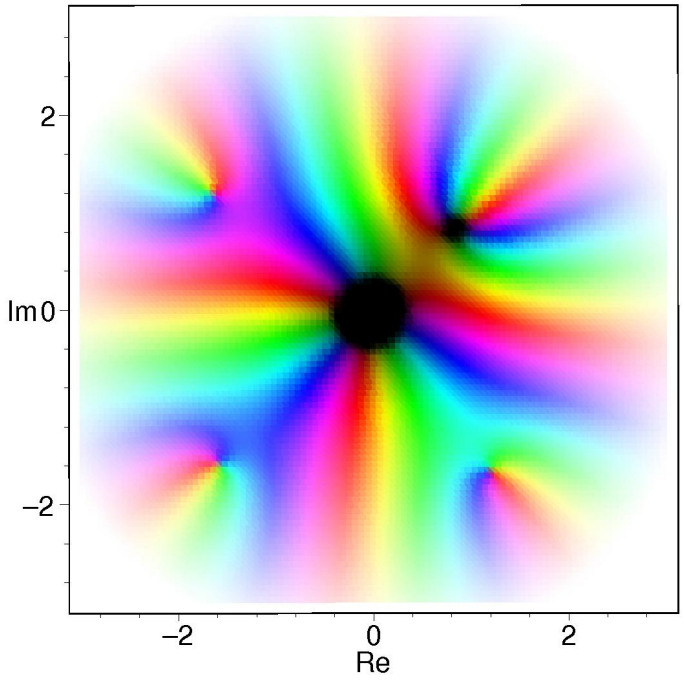
Az algebra alaptétele

3.44. 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.

Hatodik házi feladat az előadásra: második nem-bizonyítás

Tekintsük az $f = x^5 + x^2 + x + 9 + 8i \in \mathbb{C}[x]$ polinomot. Készítsen Mathematica vizualizációt, amely ábrázolja a 0 körüli r sugarú kör f melletti képét, vagyis a $G_r := \{f(z) \mid z \in \mathbb{C}, |z| = r\}$ halmazt. Az $r \in \mathbb{R}^+$ paramétert dinamikusan lehessen változtatni. Az ábra alapján röviden és informálisan válaszoljon az alábbi kérdésekre (a válaszokat is a Mathematica fájlba írva):

1. Hogyan fest a G_r görbe a sugár nagyon kicsi (pl. $r < 0,5$) értékeire?
2. Vajon miért így fest, és miért látnánk hasonlót tetszőleges f polinom esetén?
3. Hogyan fest a G_r görbe a sugár nagyon nagy (pl. $r > 3$) értékeire?
4. Vajon miért így fest, és miért látnánk hasonlót tetszőleges f polinom esetén?
5. Hogyan lehetne a fentiek alapján megmagyarázni, hogy miért van gyöke minden legalább elsőfokú $f \in \mathbb{C}[x]$ polinomnak a komplex számok körében?

- beküldendő emailben: `twaldha@math.u-szeged.hu`
- Mathematica notebook legyen
- fájlnév: `EHA-eahf6.nb` (például `WATHAAS-eahf6.nb`)
- határidő: november 2, reggel 8 óra

Irreducibilis polinomok a komplex számtest felett

3.45. 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

3.46. 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

3.47. 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. □

Gyökök és együtthatók közötti összefüggés

3.48. Tétel (Viète-formulák).

Legyenek az n-edfokú $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ főpolinom komplex gyökei $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása). Ekkor fennállnak az alábbi összefüggések:

$$
\begin{aligned}
-a_{n-1} &= \alpha_1 + \alpha_2 + \cdots + \alpha_n; \\
a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n; \\
-a_{n-3} &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n; \\
&\vdots \\
(-1)^{n-1} a_1 &= \alpha_1\alpha_2\cdots\alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2\cdots\alpha_{n-2}\alpha_n + \cdots + \alpha_2\alpha_3\cdots\alpha_{n-1}\alpha_n; \\
(-1)^n a_0 &= \alpha_1\alpha_2\alpha_3\cdots\alpha_{n-1}\alpha_n.
\end{aligned}
$$

Viète-formulák

3.49. Megjegyzés.

A fenti képleteket *Viète-formuláknak* hívjuk. A k-adik sor bal oldalán $(-1)^k a_{n-k}$ áll, a jobb oldalon pedig az $\alpha_1, \ldots, \alpha_n$ betűkből képezett összes k-tényezős szorzat összege, tehát egy $\binom{n}{k}$-tagú összeg. Formálisan:

$$(-1)^k a_{n-k} = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} \alpha_{i_1} \cdot \alpha_{i_2} \cdot \ldots \cdot \alpha_{i_k}.$$

Még formálisabban:

$$(-1)^k a_{n-k} = \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I|=k}} \prod_{i \in I} \alpha_i.$$

A Viète-formulák alkalmazása

Anélkül, hogy megkeresné a gyököket, határozza meg az $f = x^3 - 3x^2 + x - 8$ polinom gyökeinek számtani, mértani és harmonikus közepét, valamint köbösszegét.

A Viète-formulák szerint

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 3, \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= 1, \\ \alpha_1\alpha_2\alpha_3 &= 8. \end{aligned}$$

számtani közép:

$$\frac{\alpha_1 + \alpha_2 + \alpha_3}{3} = \frac{3}{3} = 1$$

mértani közép:

$$\sqrt[3]{\alpha_1\alpha_2\alpha_3} = \sqrt[3]{8} = 2$$

harmonikus közép:

$$\frac{3}{\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3}} = \frac{3}{\frac{\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3}{\alpha_1\alpha_2\alpha_3}} = \frac{3\alpha_1\alpha_2\alpha_3}{\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3} = \frac{3 \cdot 8}{1} = 24$$

A Viète-formulák alkalmazása

Példa (folyt.).

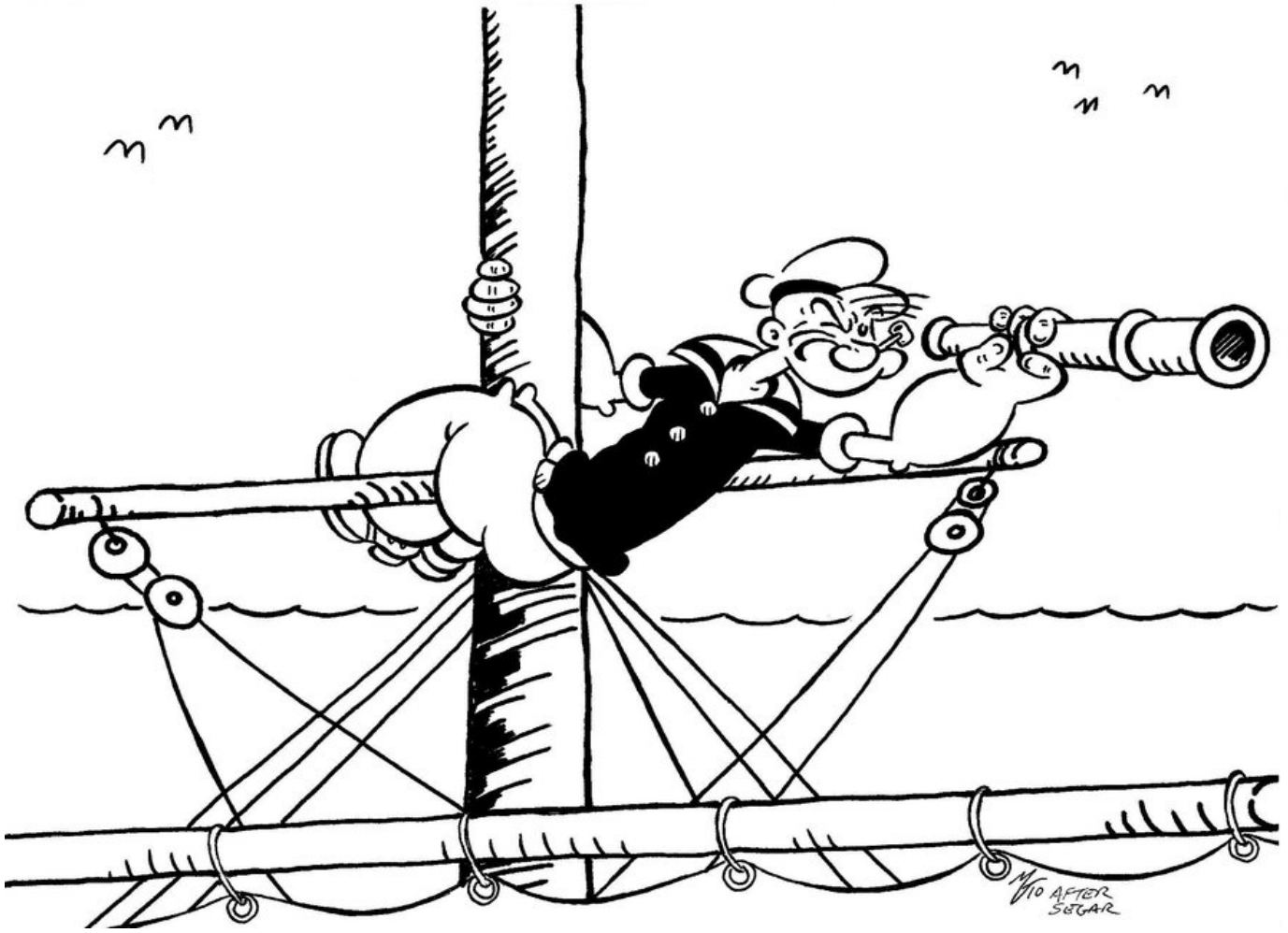
Vegyük észre, hogy

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 =$$
$$= (\alpha_1 + \alpha_2 + \alpha_3)^3 - 3 \cdot (\alpha_1 + \alpha_2 + \alpha_3) \cdot (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) + 3 \cdot \alpha_1\alpha_2\alpha_3 =$$
$$= 3^3 - 3 \cdot 3 \cdot 1 + 3 \cdot 8 = 42$$

A gyököknek a Viète-formulákban szereplő kifejezései mind szimmetrikusak, ezért bármi, amit ezek segítségével felírunk, ugyancsak szimmetrikus lesz.

A gyökök szimmetrikus polinomjait viszont mind ki lehet számítani a Viète-formulák segítségével, mert ...

Kitekintés: szimmetrikus polinomok



A szimmetrikus polinomok alaptétele

Tétel (a szimmetrikus polinomok alaptétele).

Bármely test feletti n-határozatlanú szimmetrikus polinom felírható, mégpedig egyetlen módon, az alábbi $\sigma_1, \ldots, \sigma_n$ elemi szimmetrikus polinomok polinomjaként:

$$\sigma_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_k} = \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I| = k}} \prod_{i \in I} x_i \in T\left[x_1, \ldots, x_n\right].$$

Példa.

Fejezzük ki az $(x_1 - x_2)^2$ polinomot a $\sigma_1 = x_1 + x_2$ és $\sigma_2 = x_1 x_2$ elemi szimmetrikus polinomok segítségével:

$$(x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2 = \left(x_1^2 + 2x_1x_2 + x_2^2\right) - 4x_1x_2 = \sigma_1^2 - 4\sigma_2.$$

Alkalmazzuk ezt az $ax^2 + bx + c = a\left(x - \alpha_1\right)\left(x - \alpha_2\right)$ másodfokú polinomra ...

Megoldóképlet

Példa (folyt.).

Alkalmazzuk ezt az $ax^2 + bx + c = a(x - \alpha_1)(x - \alpha_2)$ másodfokú polinomra:

$$(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = \left(\frac{-b}{a}\right)^2 - 4\frac{c}{a} = \frac{b^2 - 4ac}{a^2}.$$

Tehát

$$\left.\begin{array}{rcl} \alpha_1 - \alpha_2 & = & \frac{\sqrt{b^2-4ac}}{a} \\ \alpha_1 + \alpha_2 & = & \frac{-b}{a} \end{array}\right\} \Longrightarrow \alpha_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

Amikor egy magasabb fokú egyenletet meg akarunk oldani, akkor a nem szimmetrikus α_1 kifejezést kell felírnunk a polinom együtthatói segítségével.
A fenti példában egy négyzetgyökvonással sikerült „megtörnünk” a szimmetriát.
Legfeljebb negyedfokú polinomokra ezt meg lehet tenni, de ötödfokú polinom esetén már a gyökök szimmetriának (vagyis az S_5 permutációcsoportnak) olyan a szerkezete, hogy ez nem lehetséges.

Tétel (Ruffini, 1799; Abel, 1824; Galois, 1830).

Az általános n-edfokú egyenletnek $n \geq 5$ esetén nincs megoldóképlete, sőt, például az $x^5 - 4x + 2 = 0$ egyenletnek még „ad hoc” megoldóképlete sincs.

Valós polinom komplex gyökei

3.50. 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

3.51. 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.

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

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

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

Házi feladat a gyakorlatra

20. feladat. Határozza meg az f polinom irreducibilis felbontását $\mathbb{C}$ és $\mathbb{R}$ felett.

(a) $x^6 - 27$

$\mathbb{C}$ felett: $(x-\sqrt{3})(x+\sqrt{3})\,(x-\alpha)\,(x-\overline{\alpha})\,(x-\beta)\,(x-\overline{\beta})$,
ahol $\alpha = \frac{\sqrt{3}}{2} + \frac{3}{2}i$, $\beta = -\frac{\sqrt{3}}{2} + \frac{3}{2}i$;
$\mathbb{R}$ felett: $(x-\sqrt{3})(x+\sqrt{3})\left(x^2-\sqrt{3}x+3\right)\left(x^2+\sqrt{3}x+3\right)$

(b) $x^4 - x^2 + 1$

$\mathbb{C}$ felett: $(x-\alpha)\,(x-\overline{\alpha})\,(x-\beta)\,(x-\overline{\beta})$, ahol $\alpha = \frac{\sqrt{3}}{2} + \frac{1}{2}i$, $\beta = -\frac{\sqrt{3}}{2} + \frac{1}{2}i$;
$\mathbb{R}$ felett: $\left(x^2-\sqrt{3}x+1\right)\left(x^2+\sqrt{3}x+1\right)$

(c) $x^4 + 4$

(d) $x^7 + 7x^4 - 8x$

(e) $x^4 + x^2 - 30$

Irreducibilis polinomok $\mathbb{Q}$ felett

Ferdinand Gotthold Max Eisenstein

(1823, Berlin – 1852, Berlin)

Primitív polinomok

Példa.

$$f = \frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2} = \frac{60}{28}x^2 + \frac{315}{28}x + \frac{70}{28}$$

$$= \frac{1}{28} \cdot \left(60x^2 + 315x + 70\right) = \underbrace{\frac{5}{28}}_{r} \cdot (\underbrace{12x^2 + 63x + 14}_{f^*})$$

3.52. Definíció.

Az $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomot *primitív polinomnak* nevezzük, ha együtthatói relatív prímek, azaz $\text{lnko}(a_0, \ldots, a_n) = 1$.

3.53. Állítás.

Minden racionális együtthatós polinom felbontható egy racionális szám és egy primitív polinom szorzatára: $\forall f \in \mathbb{Q}[x] \ \exists r \in \mathbb{Q} \ \exists f^* \in \mathbb{Z}[x] : f = r \cdot f^*$ és f^* primitív polinom.

3.54. Megjegyzés.

Az előző állításban $f \sim f^*$ (ha $f \neq 0$), tehát $\mathbb{Q}[x]$-ben asszociáltság erejéig mindig lehet primitív polinomokkal számolni.

Primitív polinomok

Bizonyítás.

Legyen $f = \sum_{i=0}^{n} \frac{p_i}{q_i} \cdot x^i$, ahol $p_i, q_i \in \mathbb{Z}$, $\operatorname{lnko}(p_i, q_i) = 1 \ \ (i = 0, \ldots, n)$.

$$f = \frac{1}{Q} \cdot \sum_{i=0}^{n} \underbrace{\frac{Q}{q_i} p_i}_{b_i \in \mathbb{Z}} \cdot x^i, \quad \text{ahol } Q = \operatorname{lkkt}(q_0, \ldots, q_n)$$

$$f = \frac{d}{Q} \cdot \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i, \qquad \text{ahol } d = \operatorname{lnko}(b_0, \ldots, b_n)$$

Tehát $f = r \cdot f^*$, ahol $r = \frac{d}{Q} \in \mathbb{Q}$ és $f^* = \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i \in \mathbb{Z}[x]$ primitív polinom. □

Racionális gyökök

3.62. Tétel (Rolle(?) tétele).

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és lnko $(p, q) = 1$), akkor

$$f\left(\frac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

Természetesen a fenti nyíl nem fordítható meg: $q \mid a_n$ és $p \mid a_0$ nem garantálja, hogy $\frac{p}{q}$ gyöke f-nek.

A Rolle-tételben „az a jó”, hogy egy véges halmazt ad meg, amelyben az összes racionális gyököt megtalálhatjuk (ha van egyáltalán racionális gyök).

Racionális gyökök

Bizonyítás.

Tegyük fel, hogy $\frac{p}{q}$ gyöke f-nek (Inko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1}}_{p \mid} + \underbrace{a_0 q^n}_{p \mid} \implies p \mid a_0$$

Hasonlóan:

$$q \mid a_n \impliedby \underbrace{a_n p^n}_{q \mid} + \underbrace{a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n}_{q \mid} = 0$$

□

Irreducibilis felbontás $\mathbb{Q}$ felett

Példa.

Bontsa $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az alábbi polinomot:

$$f = 2x^5 + 3x^4 - 7x^3 - 3x^2 + 8x - 12.$$

Racionális gyök csak $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm \frac{1}{2}, \pm \frac{3}{2}$ lehet.
Ezek közül -2 kétszeres gyök, $\frac{3}{2}$ pedig egyszeres gyök:

$$f = (x - (-2))^2 \left(x - \frac{3}{2}\right)(2x^2 - 2x + 2) = (x+2)^2 (2x - 3)(x^2 - x + 1).$$

A kék polinom irreducibilis $\mathbb{Q}$ felett: csak másodfokú, és nincs racionális gyöke.

Házi feladat a gyakorlatra

21. feladat. Keresse meg az alábi polinomok öszes racionális gyökét.

(a) $2x^5 + 3x^4 - 7x^3 - 3x^2 + 8x - 12$

racionális gyökök: $-2, -2, \frac{3}{2}$, felbontás: $(x+2)^2 (2x-3) (x^2 - x + 1)$

(b) $x^6 + x^5 + 2x^4 + 4x^3 - 4x^2 + 4x - 8$

racionális gyökök: $1, -2$, felbontás: $(x-1) (x+2) (x^2+2)^2$

(c) $x^4 + 3x^3 - 3x^2 - 11x - 6$

(d) $x^6 - x^5 - 2x^3 - 3x^2 - x - 2$

(e) $x^5 + x^4 - 6x^3 - 14x^2 - 11x - 3$