

Irreducibilis polinomok \mathbb{Q} felett

Racionális gyökök

Tétel (Rolle(?) tétele).

Legyen $f = a_n x^n + \dots + a_1 x + a_0$ 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 $p \perp q$), 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).

Irreducibilis felbontás \mathbb{Q} felett

Példa.

Bontsuk \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.

Felbontás \mathbb{Q} , illetve \mathbb{Z} felett

Példa.

$$\begin{aligned} & 72x^5 - 102x^4 - 2244x^3 + 208x^2 - 1036x - 280 = \\ = & \left(\frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2} \right) \cdot \left(\frac{168}{5}x^3 - 224x^2 + \frac{448}{5}x - 112 \right) = \\ = & \frac{5}{28} (12x^2 + 63x + 14) \cdot \frac{56}{5} (3x^3 - 20x^2 + 8x - 10) = \\ = & \frac{5}{28} \frac{56}{5} \cdot (12x^2 + 63x + 14) (3x^3 - 20x^2 + 8x - 10) = \\ = & 2 \cdot (12x^2 + 63x + 14) (3x^3 - 20x^2 + 8x - 10) = \\ = & (24x^2 + 126x + 28) \cdot (3x^3 - 20x^2 + 8x - 10) \end{aligned}$$

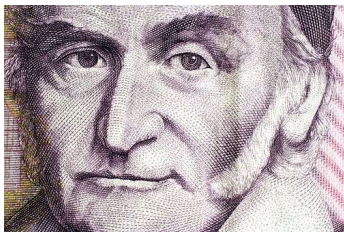
Felbontás \mathbb{Q} , illetve \mathbb{Z} felett

Tétel.

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor \mathbb{Q} felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

- (1) $\nexists g, h \in \mathbb{Z}[x] : f = gh$ és $0 < \deg g, \deg h < n$;
- (2) $\nexists g, h \in \mathbb{Q}[x] : f = gh$ és $0 < \deg g, \deg h < n$.

Bizonyítás.



Felbontás \mathbb{Q} , illetve \mathbb{Z} felett

Tétel.

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor \mathbb{Q} felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

$$(1) \nexists g, h \in \mathbb{Z}[x] : f = gh \text{ és } 0 < \deg g, \deg h < n;$$

$$(2) \nexists g, h \in \mathbb{Q}[x] : f = gh \text{ és } 0 < \deg g, \deg h < n.$$

Megjegyzés.

Mivel \mathbb{Q} test, ezért $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, tehát $\mathbb{Q}[x]$ egységei a nemnulla konstans polinomok. Ebből következik, hogy az alábbi két feltétel ekvivalens minden n -edfokú $f \in \mathbb{Q}[x]$ polinom esetén:

$$(2) \nexists g, h \in \mathbb{Q}[x] : f = gh \text{ és } 0 < \deg g, \deg h < n;$$

(2') f irreducibilis \mathbb{Q} felett.

Felbontás \mathbb{Q} , illetve \mathbb{Z} felett

Tétel.

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor \mathbb{Q} felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

$$(1) \nexists g, h \in \mathbb{Z}[x] : f = gh \text{ és } 0 < \deg g, \deg h < n;$$

$$(2) \nexists g, h \in \mathbb{Q}[x] : f = gh \text{ és } 0 < \deg g, \deg h < n.$$

Megjegyzés (folyt.).

Viszont \mathbb{Z} nem test, hiszen $\mathbb{Z}^* = \{1, -1\}$, tehát $\mathbb{Z}[x]$ -ben csak a konstans 1 és konstans -1 polinomok egységek. Ezért az alábbi két feltétel **NEM** ekvivalens minden n -edfokú $f \in \mathbb{Z}[x]$ polinom esetén:

$$(1) \nexists g, h \in \mathbb{Z}[x] : f = gh \text{ és } 0 < \deg g, \deg h < n;$$

(1') f irreducibilis \mathbb{Z} felett.

Például az $f = 2x$ polinomra (1) teljesül, de (1') nem, mert $\mathbb{Z}[x]$ -ben az $f = 2 \cdot x$ felbontás nem triviális (hiszen se 2 se x nem egység $\mathbb{Z}[x]$ -ben).

Felbontás \mathbb{Q} , illetve \mathbb{Z} felett

Tétel.

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor \mathbb{Q} felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

$$(1) \nexists g, h \in \mathbb{Z}[x] : f = gh \text{ és } 0 < \deg g, \deg h < n;$$

$$(2) \nexists g, h \in \mathbb{Q}[x] : f = gh \text{ és } 0 < \deg g, \deg h < n.$$

Megjegyzés (folyt.).

Tehát a fenti tételt **NEM** fogalmazhatjuk meg egyszerűen úgy, hogy bármely $f \in \mathbb{Z}[x]$ polinom akkor és csak akkor irreducibilis \mathbb{Q} felett, ha irreducibilis \mathbb{Z} felett.

Ez a tétel mégis jól használható \mathbb{Q} feletti irreducibilitás vizsgálatára. Adott $f \in \mathbb{Z}[x]$ polinom esetén azt kell eldöntenünk, hogy f felbomlik-e két kisebb fokszámú **egész** együtthatós polinom szorzatára. Ehhez pedig oszthatósági feltételeket lehet használni...

Kronecker módszere

Példa.

Irreducibilis-e az $f = x^4 - 4x^3 + 7x^2 - 6x + 3 \in \mathbb{Q}[x]$ polinom?

Tfh. $f = g \cdot h$, ahol $g, h \in \mathbb{Z}[x]$ és $0 < \deg g \stackrel{\text{ÁMN}}{\leq} \deg h < n$.

Ekkor $\deg g \leq 2$, és minden $k \in \mathbb{Z}$ esetén $g(k) \mid f(k)$. Például

$$a := g(0) \mid f(0) = 3, \quad b := g(1) \mid f(1) = 1, \quad c := g(2) \mid f(2) = 3.$$

Tehát az (a, b, c) számhármásra 32 lehetőség van:

$$(a, b, c) \in \{-3, -1, 1, 3\} \times \{-1, 1\} \times \{-3, -1, 1, 3\}.$$

Mind a 32 esetben egyértelműen meg tudjuk határozni a g polinomot Lagrange-interpolációval.

Ha valamelyik osztja f -et, akkor kapunk egy nemtriviális felbontást; ha egyik se osztja f -et, akkor f irreducibilis.

$$(a, b, c) = (1, 1, 3) \rightsquigarrow g = x^2 - x + 1 \rightsquigarrow f = (x^2 - x + 1)(x^2 - 3x + 3)$$

Pontos oszthatóság

Definíció.

Azt mondjuk, hogy a p prímszám *pontos osztója* az a egész számnak, ha a osztható p -vel, de p^2 -tel már nem.

Jelölés.

A pontos oszthatóságot \parallel jelöli: $p \parallel a \iff p \mid a$ és $p^2 \nmid a$.

Példa.

$$3 \parallel 12 \quad \text{de} \quad 2 \nparallel 12$$

Schönemann–Eisenstein

Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium).

Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n, p \mid a_{n-1}, \dots, p \mid a_1, p \parallel a_0,$$

akkor f irreducibilis a racionális számok teste felett.

Következmény.

Minden $n \geq 1$ egész számra létezik \mathbb{Q} felett irreducibilis n -edfokú polinom.

Bizonyítás.

$$x^n + 2$$



Érdemes ezt összehasonlítani a komplex és a valós számtest esetével:

- ▶ \mathbb{C} felett csak az elsőfokúak,
- ▶ \mathbb{R} felett csak az elsőfokúak és bizonyos másodfokúak

irreducibilisek.

VIZSGÁN KÉRDEZNI FOGOM!

Megjegyzés.

A Schönemann–Eisenstein-tétel megfordítása...

NEM IGAZ!!!

Vagyis abból, hogy nem létezik olyan p prímszám, ami teljesítené a megfelelő oszthatósági feltételeket, **nem következik**, hogy a polinom nem irreducibilis (keressünk ellenpéldát!).

A megfordítás helyett következzen inkább a tétel „tükörképe”.

Tétel (Schönemann–Eisenstein-tétel megfordítása).

Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre $p \mid a_n, p \mid a_{n-1}, \dots, p \mid a_1, p \nmid a_0$, akkor f irreducibilis a racionális számok teste felett.

Irreducibilis felbontás \mathbb{Q} felett

Példa.

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

$$f = 2x^7 + 5x^6 + 4x^5 + 13x^4 + 54x^3 + 84x^2 + 54x + 12.$$

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 -1 és $-\frac{1}{2}$ valóban gyök. Horner-módszerrel leválasztva a gyöktényezőket azt kapjuk, hogy

$$f = \left(x + \frac{1}{2}\right) (x + 1)^2 (2x^4 + 12x + 24) = (2x + 1) (x + 1)^2 (x^4 + 6x + 12).$$

A **kék** polinom irreducibilis \mathbb{Q} felett: Schönemann-Eisenstein ($p = 3$).

Példa.

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

$$f = 3x^{100} - 10x^{50} + 100x - 50.$$

A polinom irreducibilis \mathbb{Q} felett: Schönemann-Eisenstein ($p = 2$).