Irreducibilis polinomok $\mathbb{Q}$ felett

Racionális gyökök

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 $\text{lnko}\,(p, q) = 1$), 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).

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.

Primitív polinomok

Bármely $\mathbb{Q}$ feletti polinomból tudunk $\mathbb{Z}$ feletti polinomot csinálni a fellépő törtek közös nevezőjének kiemelésével.

Példa.

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

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

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 $\text{lnko}(a_0, \ldots, a_n) = 1$.

Állítás.

Minden racionális együtthatós polinom felbontható egy racionális szám és egy primitív polinom szorzatára:

$$\forall f \in \mathbb{Q}[x] \;\; \exists r \in \mathbb{Q} \; \exists f^* \in \mathbb{Z}[x] : \;\; f = r \cdot f^* \;\; \text{és} \;\; f^* \text{ primitív polinom.}$$

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

Megjegyzés.

Az előző állításban $f \sim f^*$ (ha $f \neq 0$), tehát $\mathbb{Q}[x]$-ben asszociáltság erejéig mindig lehet egész együtthatós (sőt, primitív) polinomokkal számolni. Minket a $\mathbb{Q}$ feletti irreducibilitás érdekel, ezért jó lenne kapcsolatot találni a $\mathbb{Q}$ feletti felbontások és a $\mathbb{Z}$ feletti felbontások között.

Példa.

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

Gauss-lemma

Tétel (Gauss-lemma).

Primitív polinomok szorzata is primitív.

Példa.

$$\underbrace{72x^5 - 102x^4 - 2244x^3 + 208x^2 - 1036x - 280}_{f} =$$

$$= \underbrace{\left(\frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2}\right)}_{g} \cdot \underbrace{\left(\frac{168}{5}x^3 - 224x^2 + \frac{448}{5}x - 112\right)}_{h} =$$

$$= \underbrace{\frac{5}{28}}_{r}\underbrace{(12x^2 + 63x + 14)}_{g^*} \cdot \underbrace{\frac{56}{5}}_{s}\underbrace{(3x^3 - 20x^2 + 8x - 10)}_{h^*} =$$

$$= \underbrace{\frac{5}{28}\frac{56}{5}}_{rs} \cdot \underbrace{(12x^2 + 63x + 14)(3x^3 - 20x^2 + 8x - 10)}_{g^*h^*} =$$

$$= \underbrace{\frac{p}{q}}_{\text{egyszerűsített}} \cdot \underbrace{(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)}_{\text{primitív}} \in \mathbb{Z}[x]$$

$\Longrightarrow$ $q = 1$ és $f = pg^* \cdot h^*$ (ez már egy $\mathbb{Z}$ feletti felbontás)

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 $0 < \deg g, \deg h < n$.

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

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

(2) $\nexists g, h \in \mathbb{Q}[x] : f = gh$ 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. (Meg lehet mutatni, hogy a $\mathbb{Z}$ feletti irreducibilis polinomok éppen a $\mathbb{Q}$ felett irreducibilis primitív polinomok, valamint a prímszámok, mint konstans polinomok.)

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 $0 < \deg g \overset{\text{ÁMN}}{\leq} \deg h < n$.

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) számhármasra 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 $\|$ jelöli: $p \,\|\, a \iff p \mid a$ és $p^2 \nmid a$.

Példa.

$$3 \,\|\, 12 \quad \text{de} \quad 2 \nparallel 12$$

Schönemann–Eisenstein

Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium).

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

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

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 következzék inkább a tétel „tükörképe”.

Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium).

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre $p \parallel a_n$, $p \mid a_{n-1}, \ldots, p \mid a_1$, $p \nmid a_0$, 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

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

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 ($p = 2$).