Irreducibilis polinomok

Irreducibilitás különböző testek felett

- $f \in \mathbb{C}[x]$ irreducibilis $\mathbb{C}$ felett $\iff$ $\deg f = 1$.
- $f \in \mathbb{R}[x]$ irreducibilis $\mathbb{R}$ felett $\iff$
  1. $\deg f = 1$, vagy
  2. $\deg f = 2$ és f-nek nincs valós gyöke.
- $f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ felett $\iff$???
- $f \in \mathbb{Z}_p[x]$ irreducibilis $\mathbb{Z}_p$ felett $\iff$???

Irreducibilis felbontás $\mathbb{Z}_p$ felett

5.7(d) feladat.

Bontsuk $\mathbb{Z}_5$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = x^5 + x^4 + 2x^2 + 4 \in \mathbb{Z}_5[x].$$

Megoldás.

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:

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

Ha az $x^3 + x + 1$ polinom nem lenne irreducibilis, akkor egy elsőfokú és egy másodfokú polinom szorzatára bomlana, és így lenne gyöke. De nincs neki gyöke $\mathbb{Z}_5$-ben (ha lenne, megtaláltuk volna), tehát a fenti felbontás az f polinom irreducibilis faktorizációja.

Irreducibilitás vs. gyökök

Legyen T tetszőleges test és $f \in T[x]$.

- $\deg f = 1$ esetén:

  f irreducibilis T felett.

- $\deg f = 2$ esetén:

  f akkor és csak akkor irreducibilis T felett, ha nincs gyöke T-ben.

- $\deg f = 3$ esetén:

  f akkor és csak akkor irreducibilis T felett, ha nincs gyöke T-ben.

- $\deg f \geq 4$ esetén:

  ha f-nek van gyöke T-ben, akkor nem irreducibilis T felett,
  de ha nincs gyöke, akkor bármi megtörténhet.

Irreducibilitás vs. gyökök

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM NEM NEM NEM NEM NEM NEM

KÖVETKEZIK

AZ IRREDUCIBILITÁS!!!

Irreducibilis felbontás $\mathbb{Z}_p$ felett

5.7(e) feladat.

Bontsuk $\mathbb{Z}_5$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

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

Megoldás.

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:

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

Az $x^2 + 4x + 2$ polinomnak nincs gyöke $\mathbb{Z}_5$-ben (ha lenne, megtaláltuk volna), és csak másodfokú, ezért irreducibilis $\mathbb{Z}_5$ felett.

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

Racionális gyökök

Tétel (Rolle(?) tétele).

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

5.7(f) feladat.

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

$$f = x^5 + 2x^4 - 3x^3 + 2x^2 + 4x - 6 \in \mathbb{Q}[x].$$

Megoldás.

Rolle: racionális gyök csak $\pm 1, \pm 2, \pm 3, \pm 6$ lehet.

Ezek közül 1 és -3 valóban gyök. Horner-módszerrel leválasztva a gyöktényezőket azt kapjuk, hogy

$$f = (x-1) \cdot \big(x - (-3)\big) \cdot (x^3 + 2) = (x-1) \cdot (x+3) \cdot (x^3 + 2).$$

Az $x^3 + 2$ polinomnak nincs racionális gyöke (ha lenne, megtaláltuk volna), és csak harmadfokú, ezért irreducibilis $\mathbb{Q}$ felett.

Irreducibilis felbontás $\mathbb{Q}$ felett

5.7(g) feladat.

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

$$f = 2x^5 + 3x^4 - 7x^3 - 3x^2 + 8x - 12 \in \mathbb{Q}[x].$$

Megoldás.

Rolle: 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 és $\frac{3}{2}$ valóban gyök. Horner-módszerrel leválasztva a gyöktényezőket azt kapjuk, hogy

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

$$= (x+2)^2 \cdot (2x-3) \cdot (x^2 - x + 1).$$

Az $x^2 - x + 1$ polinomnak nincs racionális gyöke (ha lenne, megtaláltuk volna), és csak másodfokú, ezért irreducibilis $\mathbb{Q}$ felett.

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 prím, amelyre

$$p \nmid a_n,\, p \mid a_{n-1}, \ldots, p \mid a_1,\, p \mid a_0,\, p^2 \nmid a_0,$$

akkor f irreducibilis a racionális számok teste felett.

Következmény.

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

Bizonyítás.

$x^n + 2$ $\square$

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.

Irreducibilis felbontás $\mathbb{Q}$ felett

5.8(d) feladat.

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

$$f = x^6 + 8x^5 + 13x^4 + 10x^3 + 10x^2 + 8x + 2 \in \mathbb{Q}[x].$$

Megoldás.

Rolle: racionális gyök csak $\pm 1, \pm 2$ lehet.

Ezek közül -1 valóban gyök. Horner-módszerrel leválasztva a gyöktényezőket azt kapjuk, hogy

$$f = \big(x - (-1)\big)^2 \cdot (x^4 + 6x^3 + 4x + 2) = (x+1)^2 \cdot (x^4 + 6x^3 + 4x + 2).$$

Az $x^4 + 6x^3 + 4x + 2$ polinom már irreducibilis $\mathbb{Q}$ felett: Schönemann-Eisenstein ($p = 2$).

5.8(e) feladat.

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

$$f = 3x^{100} - 10x^{50} + 100x - 20.$$

Megoldás.

A polinom irreducibilis $\mathbb{Q}$ felett: Schönemann-Eisenstein ($p = 5$).

Schönemann–Eisenstein-féle irreducibilitási kritérium

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.