Irreducibilis polinomok

Irreducibilitás

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:

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

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

□

Egyértelmű irreducibilis faktorizáció

Definíció.

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

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

Tétel.

Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.

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

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

Irreducibilitás vs. gyökök

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. □

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

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!!!

Irreducibilis faktorizáció

Példa.

Bontsa 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 . . .)

Polinomgyűrű maradékosztályteste

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 (3.25. Áll.);
2. $\overline{f}$-nak akkor és csak akkor van inverze, ha $f \perp m$ (3.26. Tétel);
3. tehát $T[x]/(m)$ akkor és csak akkor test, ha legalább kételemű, és

$$(*) \qquad \forall f \in T[x]: \; m \nmid f \implies f \perp m$$

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

□

Legyen $m = x^2 + x + 1 \in \mathbb{Z}_2[x]$ (miért irreducibilis?).
A $T := \mathbb{Z}_2[x]/(m)$ testnek négy eleme van: $\overline{0}$, $\overline{1}$, $\overline{x}$, $\overline{x+1}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Ugyanez tömörebben, a $0 := \overline{0}$, $1 := \overline{1}$, $\alpha := \overline{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Figyeljük meg, hogy

- $\{0, 1\} = \{\overline{0}, \overline{1}\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot T-ben;
- $\alpha = \overline{x}$ gyöke az $x^2 + x + 1 \in T[x]$ polinomnak:
  $\alpha^2 + \alpha + 1 = \overline{x}^2 + \overline{x} + \overline{1} = \overline{x^2 + x + 1} = \overline{0} = 0$.

Polinomgyűrű maradékosztályteste

Tétel.

Legyen T test, $m \in T[x]$ irreducibilis polinom, és jelölje n az m polinom fokszámát. Ekkor a $K = T[x]/(m)$ maradékosztálygyűrű olyan test, amelyben az m polinomnak van gyöke: az $\alpha = \overline{x} \in K$ elemre $m(\alpha) = m(\overline{x}) = \overline{m(x)} = \overline{m} = \overline{0}$

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 $|K| = p^n$.)

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?)

Egyszerű algebrai bővítés

Következmény.

Tetszőleges T test és $m \in T[x]$ irreducibilis polinom esetén létezik olyan K test, amelyre

1. K *bővítése* T-nek, azaz $K \supseteq T$;
2. létezik olyan $\alpha \in K$ elem, amely gyöke m-nek;
3. K minden eleme egyértelműen előáll $a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$ $(a_{n-1}, \ldots, a_0 \in T)$ alakban, ahol $n = \deg m$.

Bizonyítás.

Legyen $K = T[x]/(m)$, és alkalmazzuk az előző tételt. □

Definíció.

Azt mondjuk, hogy a K test T-ből az α elem *adjungálásával* keletkezik (jelölés: $K = T(\alpha)$), és az ilyen módon előálló testeket T *egyszerű algebrai bővítéseinek* nevezzük.

A komplex számtest újratöltve

Hajtsuk végre az előbbi konstrukciót a $T = \mathbb{R}$ és $m = x^2 + 1$ esetben.
Most $n = \deg(x^2 + 1) = 2$, tehát

$$K = \left\{ \overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R} \right\}.$$

Írjunk $\overline{x}$ helyett α-t, és hagyjuk el a vonásokat a konstansokról.

Ekkor K egy tipikus eleme:

$$\overline{a_0 + a_1 x} = \overline{a_0} + \overline{a_1} \cdot \overline{x} = a_0 + a_1 \cdot \alpha,$$

és az α szimbólumra vonatkozó (egyetlen) számolási szabály: $\alpha^2 = -1$.

Tehát $\mathbb{R}[x] / \left(x^2 + 1\right) \cong \mathbb{C}$, és ezt tekinthetnénk akár a komplex számok definíciójának is.

Egy végtelen maradékosztálytest

Példa.

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

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.

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.

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

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

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

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.

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

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

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

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

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

$\Longrightarrow$ $q = 1$ 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

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

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 ($p = 2$).

Elemi törtekre bontás

Elemi törtekre bontás a racionális számok körében

Definíció.

Elemi törteknek nevezzük a $\frac{c}{p^k}$ alakú törteket, ahol p prímszám, k és c pozitív egészek, és $c < p$.

Tétel.

Minden racionális szám felírható egy egész szám és elemi törtek összegeként.

Bizonyítás (vázlat).

Három „trükkre” lesz szükségünk:

1. Tetszőleges $a, b, c \in \mathbb{Z}\,(a, b \neq 0)$ esetén

$$a \perp b \implies \exists x, y \in \mathbb{Z}: \ \frac{c}{ab} = \frac{x}{a} + \frac{y}{b}.$$

Ezt ismételten alkalmazva minden racionális számot fel tudunk bontani prímhatvány nevezőjű törtek összegére. Például:

$$\frac{157}{72} = \frac{157}{2^3 \cdot 3^2} = \frac{x}{2^3} + \frac{y}{3^2} = \frac{21}{2^3} + \frac{-4}{3^2}.$$

Elemi törtekre bontás a racionális számok körében

Bizonyítás (folyt.)

2. Maradékos osztás segítségével leválasztva a törtek egészrészét, elérhetjük, hogy minden törtünk $\frac{c}{p^k}$ alakú legyen, ahol $0 < c < p^k$:

$$\frac{157}{72} = \frac{21}{2^3} + \frac{-4}{3^2} = 2 + \frac{5}{2^3} + (-1) + \frac{5}{3^2} = 1 + \frac{5}{2^3} + \frac{5}{3^2}.$$

3. Minden $\frac{c}{p^k}$ alakú törtben a számlálót felírjuk p-alapú számrendszerben, és „számjegyenként szétszedjük”:

$$\frac{5}{2^3} = \frac{101_2}{2^3} = \frac{2^2+1}{2^3} = \frac{2^2}{2^3} + \frac{1}{2^3} = \frac{1}{2} + \frac{1}{2^3};$$

$$\frac{5}{3^2} = \frac{12_3}{3^2} = \frac{3+2}{3^2} = \frac{3}{3^2} + \frac{2}{3^2} = \frac{1}{3} + \frac{2}{3^2}.$$

Tehát a végeredmény:

$$\frac{157}{72} = 1 + \frac{1}{2} + \frac{1}{2^3} + \frac{1}{3} + \frac{2}{3^2}.$$

□

Polinomokra minden ugyanúgy megy

Tetszőleges T test esetén a $T[x]$ polinomgyűrű elemeivel „ugyanúgy” lehet számolni, mint egész számokkal (maradékos osztás, euklideszi algoritmus), ezért az előbbi eljárás T feletti polinomokra is működik.

Definíció.

A T test feletti ***racionális törtön*** $\frac{f}{g}$ alakú formális kifejezést értünk, ahol $f, g \in T[x]$ és $g \neq 0$. Minden racionális törthöz tartozik egy ***racionális törtfüggvény*** (a két fogalom nem összekeverendő!). A T feletti racionális törtek halmazát $T(x)$ jelöli.

Definíció.

A T test felett ***elemi törtnek*** (vagy parciális törtnek) olyan racionális törtet nevezünk, amelyben a nevező T felett irreducibilis (fő)polinom hatványa, és a számláló foka kisebb ezen irreducibilis polinom fokánál:

$$\frac{f}{p^k} \in T(x), \quad \text{ahol } f, p \in T[x],\ k \in \mathbb{N},\ p \text{ irreducibilis } T \text{ felett, } \deg f < \deg p.$$

Elemi törtekre bontás test feletti racionális törtek körében

Tétel.

Tetszőleges T test felett minden racionális tört felírható egy polinom és elemi racionális törtek összegeként.

Következmény.

A komplex számok teste felett minden racionális tört felírható egy polinom és véges sok

$$\frac{A}{(x+a)^k} \quad (A, a \in \mathbb{C},\ k \in \mathbb{N})$$

alakú racionális tört összegeként.

Következmény.

A valós számok teste felett minden racionális tört felírható egy polinom és véges sok

$$\frac{A}{(x+a)^k} \quad (A, a \in \mathbb{R},\ k \in \mathbb{N}), \text{ illetve}$$

$$\frac{Bx+C}{(x^2+bx+c)^k} \quad (B, C, b, c \in \mathbb{R},\ b^2-4c<0,\ k \in \mathbb{N})$$

alakú racionális tört összegeként.

Elemi törtekre bontás $\mathbb{R}$ feletti racionális törtek körében

Példa.

Bontsuk parciális törtek összegére $\mathbb{R}$ felett az $\dfrac{1}{x^2+x}$ racionális törtet.

$$\frac{1}{x^2+x} = \frac{1}{x(x+1)} = \frac{A}{x} + \frac{B}{x+1} = \frac{A(x+1)+Bx}{x(x+1)} = \frac{(A+B)x+A}{x(x+1)}$$

$$\Updownarrow$$

$$A+B=0 \text{ és } A=1$$

$$\Updownarrow$$

$$A=1 \text{ és } B=-1$$

Tehát

$$\frac{1}{x^2+x} = \frac{1}{x} - \frac{1}{x+1}.$$

Elemi törtekre bontás $\mathbb{R}$ feletti racionális törtek körében

Példa.

Bontsuk parciális törtek összegére $\mathbb{R}$ felett a $\dfrac{3x^2+2x+1}{x^7+2x^5+x^3}$ racionális törtet.

$$\frac{3x^2+2x+1}{x^7+2x^5+x^3} = \frac{3x^2+2x+1}{x^3\left(x^4+2x^2+1\right)} = \frac{3x^2+2x+1}{x^3\left(x^2+1\right)^2} =$$

$$= \frac{A}{x} + \frac{B}{x^2} + \frac{C}{x^3} + \frac{Dx+E}{x^2+1} + \frac{Fx+G}{\left(x^2+1\right)^2} =$$

$$= \frac{Ax^2\left(x^2+1\right)^2+Bx\left(x^2+1\right)^2+C\left(x^2+1\right)^2+(Dx+E)x^3\left(x^2+1\right)+(Fx+G)x^3}{x^3\left(x^2+1\right)^2} =$$

$$= \frac{(A+D)x^6+(B+E)x^5+(2A+C+D+F)x^4+(2B+E+G)x^3+(A+2C)x^2+Bx+C}{x^3\left(x^2+1\right)^2}$$

$$\Updownarrow$$

$$A+D=0,\ B+E=0,\ 2A+C+D+F=0,$$

$$2B+E+G=0,\ A+2C=3,\ B=2,\ C=1$$

Elemi törtekre bontás $\mathbb{R}$ feletti racionális törtek körében

Példa (folyt.).

A kapott hétismeretlenes lineáris egyenletrendszert megoldjuk:

$$A = 1,\ B = 2,\ C = 1,\ D = -1,\ E = -2,\ F = -2,\ G = 2.$$

Tehát

$$\frac{3x^2+2x+1}{x^7+2x^5+x^3} = \frac{1}{x} + \frac{2}{x^2} + \frac{1}{x^3} + \frac{-x-2}{x^2+1} + \frac{-2x-2}{(x^2+1)^2}.$$

Elemi törtekre bontás $\mathbb{C}$ feletti racionális törtek körében

Példa.

Bontsuk parciális törtek összegére $\mathbb{C}$ felett a $\dfrac{3x^2+2x+1}{x^7+2x^5+x^3}$ racionális törtet.

$$\frac{3x^2+2x+1}{x^7+2x^5+x^3} = \frac{3x^2+2x+1}{x^3\left(x^2+1\right)^2} = \frac{3x^2+2x+1}{x^3\left(x+i\right)^2\left(x-i\right)^2} =$$

$$= \frac{A}{x} + \frac{B}{x^2} + \frac{C}{x^3} + \frac{D}{x+i} + \frac{E}{\left(x+i\right)^2} + \frac{F}{x-i} + \frac{G}{\left(x-i\right)^2}$$

$$\Updownarrow$$

$$A+D+F=0,\ B-iD+E+iF+G=0,\ 2A+C+D-2iE+F+2iG=0,$$

$$2B-iD-E+iF-G=0,\ A+2C=3,\ B=2,\ C=1$$

Elemi törtekre bontás $\mathbb{C}$ feletti racionális törtek körében

Példa (folyt.).

A kapott hétismeretlenes lineáris egyenletrendszert megoldjuk:

$$A = 1,\ B = 2,\ C = 1,\ D = -\frac{1}{2} - \frac{3}{2}i,\ E = \frac{1}{2} - \frac{1}{2}i,\ F = -\frac{1}{2} + \frac{3}{2}i,\ G = \frac{1}{2} + \frac{1}{2}i.$$

Tehát

$$\frac{3x^2+2x+1}{x^7+2x^5+x^3} = \frac{1}{x} + \frac{2}{x^2} + \frac{1}{x^3} + \frac{-\frac{1}{2} - \frac{3}{2}i}{x+i} + \frac{\frac{1}{2} - \frac{1}{2}i}{(x+i)^2} + \frac{-\frac{1}{2} + \frac{3}{2}i}{x-i} + \frac{\frac{1}{2} + \frac{1}{2}i}{(x-i)^2}.$$