Algebra és számelmélet 3 előadás
Irreducibilis polinomok

Waldhauser Tamás
2014 őszi félév

Tartalom

1. Irreducibilis polinomok

2. Irreducibilis polinomok a racionális számtest felett

3. Elemi törtekre bontás

Tartalom

1. Irreducibilis polinomok

2. Irreducibilis polinomok a racionális számtest felett

3. Elemi törtekre bontás

Emlékeztető

Definíció vagy tétel?

Legyen T egy test és $p \in T[x]$. A p polinom **irreducibilis** T felett, ha legalább elsőfokú, és nem bontható deg p-nél kisebb fokszámú polinomok szorzatára:

$$\nexists f, g \in T[x]: \quad p = f \cdot g \quad \text{és} \quad 1 \leq \deg f, \deg g < \deg p.$$

Vigyázat!

Gyűrűk felett ez általában nem igaz! Például a $p = 2x \in \mathbb{Z}[x]$ polinom nem irreducibilis $\mathbb{Z}$ felett, mert a $p = 2 \cdot x$ felbontás itt nem triviális (miért?).

1. Tétel.

- *Az elsőfokú polinomok bármely test felett irreducibilisek.*
- *Ha* $f \in T[x]$ *irreducibilis és* $\deg f \geq 2$, *akkor* f*-nek nincs gyöke* T*-ben.*
- *Ha* $f \in T[x]$ *és* $2 \leq \deg f \leq 3$, *akkor* f *pontosan akkor irreducibilis, ha nincs gyöke* T*-ben.*

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!!!

Egy irreducibilis faktorizáció

Példa.

Bontsuk 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 . . .)

Még néhány irreducibilis faktorizáció

Példa.

Bontsuk irreducibilis tényezők szorzatára az $x^2 + x + 1$ polinomot $\mathbb{Z}_3$, $\mathbb{Z}_5$ és $\mathbb{Z}_7$ felett. $\mathbb{Z}_3$ felett $(x-1)^2$, $\mathbb{Z}_5$ felett x^2+x+1 , $\mathbb{Z}_7$ felett $(x-2)(x-4)$

Házi feladat.

Bontsa irreducibilis tényezők szorzatára az $x^4 + 3x^3 + x^2 + 4$ polinomot $\mathbb{Z}_3$, $\mathbb{Z}_5$ és $\mathbb{Z}_7$ felett.

Példa.

Határozzuk meg $\mathbb{Z}_2$ felett az összes legfeljebb harmadfokú irreducibilis polinomot.

$x,\ x+1,\ x^2+x+1,\ x^3+x+1,\ x^3+x^2+1$

Példa.

Bontsuk irreducibilis tényezők szorzatára az $x^4 + x + 1$ és $x^4 + x^2 + 1$ polinomokat $\mathbb{Z}_2$ felett. x^4+x+1 és $(x^2+x+1)^2$

Véges testek

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

Emlékeztető

3. Definíció.

Az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinom $c \in T$ helyen vett **helyettesítési értékén** az $f(c) = a_n c^n + \cdots + a_1 c + a_0 \in T$ elemet értjük.
Az $f \in T[x]$ polinomhoz tartozó **polinomfüggvény** pedig nem más, mint az

$$f : T \to T,\ c \mapsto f(c)$$

leképezés.

A polinomot és a hozzá tartozó polinomfüggvényt ugyanúgy jelöljük; a szövegkörnyezetből kiderül, hogy mikor melyikről van szó. Ha polinomfüggvényekről van szó, akkor x-et **változónak** nevezzük (nem pedig határozatlannak).

Polinom vs. polinomfüggvény

Példa.
Az $f = x^3 \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0}^3 = \overline{0},\ \overline{1} \mapsto \overline{1}^3 = \overline{1},\ \overline{2} \mapsto \overline{2}^3 = \overline{2}.$$

A $g = x \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0},\ \overline{1} \mapsto \overline{1},\ \overline{2} \mapsto \overline{2}.$$

Látjuk, hogy f-hez és g-hez ugyanaz a polinomfüggvény tartozik (nevezetesen az identikus függvény), noha f és g két különböző polinom. Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Polinom vs. polinomfüggvény

Általánosabban, ha T egy q-elemű test, akkor

- a $T \to T$ leképezések száma  q^q, míg
- T feletti polinomból  végtelen sok van,

így végtelen sok különböző polinomhoz tartozik ugyanaz a polinomfüggvény. Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Tartalom

1. Irreducibilis polinomok

2. Irreducibilis polinomok a racionális számtest felett

3. Elemi törtekre bontás

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

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

Emlékeztető

A komplex számtest felett csak az elsőfokú polinomok irreducibilisek, a valós számtest felett pedig csak az elsőfokúak és a negatív diszkriminánsú másodfokúak.

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

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

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

5. Megjegyzés.

A második feltétel azzal ekvivalens, hogy f reducibilis $\mathbb{Q}$ felett. Az első viszont *nem* ekvivalens azzal, hogy f reducibilis $\mathbb{Z}$ felett (miért?).

Tehát a fenti tételt *nem* fogalmazhatjuk meg egyszerűen úgy, hogy egy egész együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ felett, ha irreducibilis $\mathbb{Q}$ felett.

6. Megjegyzés.

Az (1) $\implies$ (2) irány világos (ugye?), a (2) $\implies$ (1) irány viszont egyáltalán nem triviális (még Gauss is kell hozzá!).

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.

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

Schönemann–Eisenstein

7. 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.

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

8. 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*

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

akkor f *irreducibilis a racionális számok teste felett.*

Irreducibilis polinomok $\mathbb{Q}$ felett

9. 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.

Még szerencse, hogy a racionális számok testének már nincs valódi részteste! 

VIZSGÁN KÉRDEZNI FOGOM!

10. 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”.

11. 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.*

Racionális gyökök

12. 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).

Racionális gyökök

Bizonyítás.

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

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

Szorozzunk be q^n-nel:

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

Hasonlóan:

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

□

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 gyökényezőket 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-Elsenstein, $p = 3$).

Irreducibilis felbontás $\mathbb{Q}$ felett

Példa.

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

- $2x^{100} - 3x^{73} + 69x - 12$; irreducibilis (SE $p = 3$)
- $x^3 + 5x^2 + 6x + 1$; irreducibilis (csak harmadfokú, és nincs racionális gyöke)
- $x^7 - 7x^6 + 24x^5 - 50x^4 + 68x^3 - 57x^2 + 25x - 1$; $y = x - 1$: $f = y^7 + 3y^5 + 3y^3 + 3y^2 + 3$ (SE $p = 3$)
- $x^6 + 125$. $\mathbb{R}$ felett $f = (x^2 + 5)\left(x^2 - \sqrt{15}x + 5\right)\left(x^2 + \sqrt{15}x + 5\right) \implies \mathbb{Q}$ felett $f = (x^2 + 5)(x^4 - 5x^2 + 25)$

Házi feladat.

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

- $4x^4 - 7x^2 - 5x - 1$;
- $5x^8 - 5x^7 + 4x^2 - 2x - 2$;
- $x^4 - x^3 + 2x + 1$ (útmutatás: térjünk át az $y = x - 1$ határozatlanra);
- $x^6 - 125$;
- $x^4 + 36$.

Tartalom

1. Irreducibilis polinomok

2. Irreducibilis polinomok a racionális számtest felett

3. Elemi törtekre bontás

Elemi törtekre bontás a racionális számok körében

13. Definíció.

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

14. 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 nevezőt 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.

15. 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.

16. 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

17. Tétel.

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

18. 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.

19. Következmény.

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

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

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

alakú racionális tört összegeként.

Elemi törtekre bontás test 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 test 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.

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

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

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

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

$$\Updownarrow$$

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

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

Elemi törtekre bontás test 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 test 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 test 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

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

Megértést ellenőrző kérdések

- Létezik-e harmadfokú irreducibilis polinom $\mathbb{Z}_2$ felett?
- Létezik-e 2014-edfokú irreducibilis polinom $\mathbb{R}$ felett?
- Igaz-e minden $f \in \mathbb{Q}[x]$ polinomra, hogy ha f irreducibilis $\mathbb{Q}$ felett, akkor f-nek nincs valós gyöke?
- Létezik-e olyan $f \in \mathbb{Q}[x]$ polinom, ami irreducibilis $\mathbb{R}$ felett, de nem irreducibilis $\mathbb{Q}$ felett?
- Igaz-e tetszőleges T testre és $f, g \in T[x]$ polinomokra, hogy ha minden $c \in T$ esetén $f(c) = g(c)$, akkor $f = g$?
- Létezik-e olyan $0 \neq f \in \mathbb{Z}[x]$ főpolinom, amelynek $\frac{1}{2}$ gyöke?
- Létezik-e olyan irreducibilis polinom $\mathbb{Q}$ felett, amelynek van racionális gyöke?
- Igaz-e tetszőleges $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomra, hogy ha nem 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 nem irreducibilis $\mathbb{Q}$ felett? Ha nem, akkor adjon meg egy ellenpéldát!