Klasszikus algebra előadás

Waldhauser Tamás
2014. március 31.

Primitív polinomok

3.51. Definíció.

Az $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomot *primitív polinom*nak nevezzük, ha együtthatói relatív prímek, azaz lnko $(a_0, \ldots, a_n) = 1$.

3.52. Állítás.

Minden racionális együtthatós polinom felbontható egy racionális szám és egy primitív polinom szorzatára: $\forall f \in \mathbb{Q}[x]\ \exists r \in \mathbb{Q}\ \exists f^* \in \mathbb{Z}[x] : f = r \cdot f^*$ *és* f^* *primitív polinom.*

3.53. Megjegyzés.

Az előző állításban $f \sim f^*$ (ha $f \neq 0$), tehát $\mathbb{Q}[x]$-ben asszociáltság erejéig mindig lehet primitív polinomokkal számolni.

Példa.

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

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

Primitív polinomok

Bizonyítás.

Legyen $f = \sum_{i=0}^{n} \frac{p_i}{q_i} \cdot x^i$, ahol $p_i, q_i \in \mathbb{Z}$, $\operatorname{lnko}(p_i, q_i) = 1 \ \ (i = 0, \ldots, n)$.

$$f = \frac{1}{Q} \cdot \sum_{i=0}^{n} \underbrace{\frac{Q}{q_i} p_i}_{b_i \in \mathbb{Z}} \cdot x^i, \quad \text{ahol } Q = \operatorname{lkkt}(q_0, \ldots, q_n)$$

$$f = \frac{d}{Q} \cdot \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i, \qquad \text{ahol } d = \operatorname{lnko}(b_0, \ldots, b_n)$$

Tehát $f = r \cdot f^*$, ahol $r = \frac{d}{Q} \in \mathbb{Q}$ és $f^* = \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i \in \mathbb{Z}[x]$ primitív polinom. □

Redukció modulo p

Jelölés.

Adott p prímszám esetén az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom modulo p redukáltján az

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x]$$

polinomot értjük, ahol $\overline{a_i}$ az a_i egész számot tartalmazó modulo p maradékosztály.

A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x]: \ \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Nyilván $\deg \overline{f} \leq \deg f$, továbbá ha $p \nmid a_n$, akkor (és csak akkor!) $\overline{a_n} \neq \overline{0}$, és így $\deg \overline{f} = \deg f = n$.

Példa.

Legyen $p = 5$ és $f = 10x^3 + 7x^2 + 25x - 2$. Ekkor

$$\overline{f} = \overline{10}x^3 + \overline{7}x^2 + \overline{25}x + \overline{-2} = \overline{0}x^3 + \overline{2}x^2 + \overline{0}x + \overline{3} = \overline{2}x^2 + \overline{3} \in \mathbb{Z}_5[x].$$

Egy trükk

Példa.

Felbontható-e az $f = x^4 + 2x^3 + 6x^2 + 7x + 5 \in \mathbb{Z}[x]$ polinom kisebb fokszámú egész együtthatós polinomok szorzatára?

Tegyük fel, hogy igen:

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \quad \text{és } 0 < \deg g, \deg h < 4.$$

Redukáljuk modulo 2: $\overline{f} = \overline{g} \cdot \overline{h}$, ahol $\overline{g} \cdot \overline{h} \in \mathbb{Z}_2[x]$ és $0 < \deg \overline{g}, \deg \overline{h} < 4$. 

Node $\overline{f} =$  $x^4 + x + 1$ irreducibilis $\mathbb{Z}_2[x]$-ben, mert  nincs neki se első- se másodfokú irreducibilis osztója. 

Tehát f nem bontható fel kisebb fokú egész együtthatós polinomok szorzatára. Nemsokára bebizonyítjuk, hogy ekkor f nem bontható fel kisebb fokú racionális együtthatós polinomok szorzatára sem, tehát irreducibilis $\mathbb{Q}$ felett.

Gauss-lemma

3.54. Lemma.

Tetszőleges $f \in \mathbb{Z}[x]$ polinom akkor és csak akkor primitív, ha minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját,  és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

3.55. Tétel (Gauss-lemma).

Primitív polinomok szorzata is primitív.

Bizonyítás.

Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

- fg nem primitív $\Longrightarrow$ létezik olyan p prím, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$.
- f és g primitív $\Longrightarrow$ $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$ és $\overline{g} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Tehát $\mathbb{Z}_p[x]$-ben $\overline{f}$ és $\overline{g}$  zérusosztók, ez pedig lehetetlen,  mivel $\mathbb{Z}_p$ test. □

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

3.56. 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* $0 < \deg g, \deg h < n$.

3.57. Megjegyzés.

A második feltétel azzal ekvivalens, hogy f reducibilis $\mathbb{Q}$ felett. Az első viszont *nem* ekvivalens azzal, hogy f reducibilis $\mathbb{Z}$ felett.
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.
Például a $2 \cdot x$ faktorizáció $\mathbb{Z}[x]$-ben nemtriviális, mert $2 \notin \mathbb{Z}[x]^*$ ezért a $2x$ polinom nem irreducibilis $\mathbb{Z}$ felett ($\mathbb{Q}$ felett viszont irreducibilis, hiszen elsőfokú).
Meg lehet mutatni, hogy a $\mathbb{Z}$ feletti irreducibilis polinomok éppen a $\mathbb{Q}$ felett irreducibilis primitív polinomok, valamint a prímszámok (mint konstans polinomok).

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

3.56. Tétel.

$\forall f \in \mathbb{Z}[x], \deg f \geq 1$ *esetén* $(1) \iff (2)$

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

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

Bizonyítás.

Az világos, hogy  $(1) \implies (2)$.
Tegyük fel, hogy (2) teljesül, és legyen

$$g = r \cdot g^*, \ h = s \cdot h^*, \text{ ahol } r, s \in \mathbb{Q} \text{ és } g^*, h^* \in \mathbb{Z}[x] \text{ primitív polinomok.}$$

Legyen $rs = \frac{p}{q}$, ahol $\text{lnko}(p, q) = 1$ és $q > 0$. Ekkor

$$f = g \cdot h = rg^* \cdot sh^* = rs \cdot g^* h^* = \frac{p}{q} \cdot g^* h^*.$$

Meg fogjuk mutatni, hogy $q = 1$.

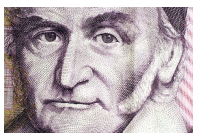
Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\begin{aligned} & \forall i \in \{0, \ldots, n\} : \ q \mid p \cdot a_i \\ \implies & \forall i \in \{0, \ldots, n\} : \ q \mid a_i \\ \implies & q \mid \operatorname{lnko}(a_0, \ldots, a_n) \\ \implies & q = 1 \end{aligned}$$



Tehát

$$f = \frac{p}{q} \cdot g^* h^* = \underbrace{pg^*}_{\in \mathbb{Z}[x]} \cdot \underbrace{h^*}_{\in \mathbb{Z}[x]}.$$

A fenti felbontásban a fokszámok ugyanazok, mint az eredeti $f = gh$ felbontásban, hiszen $pg^* \sim g$ és $h^* \sim h$. □

Pontos oszthatóság

3.58. Definíció.

Azt mondjuk, hogy a p prímszám *pontos osztó*ja 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

3.59. 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.*

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett. A 3.56. Tétel szerint

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \ \text{ és } \ 0 < \deg g, \deg h < n.$$

Redukáljunk modulo p: $\overline{f} = \overline{g \cdot h} = \overline{g} \cdot \overline{h} \in \mathbb{Z}_p[x]$. Tudjuk, hogy

$$\deg \overline{g} \leq \deg g \text{ és } \deg \overline{h} \leq \deg h.$$

Ha itt valamelyik egyenlőtlenség szigorú lenne, akkor

$$\deg \overline{f} = \deg \overline{g \cdot h} = \deg \overline{g} + \deg \overline{h} < \deg g + \deg h = \deg f = n,$$

ami  ,  hiszen $p \nmid a_n$ miatt f fokszáma nem csökken a mod p redukciónál.

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} = \overline{b} x^k, \ \overline{h} = \overline{c} x^l, \text{ ahol } k + l = n \text{ és } \overline{b} \cdot \overline{c} = \overline{a_n}.$$

Ebből következik, hogy

$$\left.\begin{array}{rcl} \overline{g(0)} = \overline{g}(\overline{0}) = \overline{b} \cdot \overline{0}^k = \overline{0} & \Longrightarrow & p \mid g(0) \\ \overline{h(0)} = \overline{h}(\overline{0}) = \overline{c} \cdot \overline{0}^l = \overline{0} & \Longrightarrow & p \mid h(0) \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow p^2 \mid g(0) \cdot h(0) = f(0) = a_0. \quad \square$$

Irreducibilis polinomok $\mathbb{Q}$ felett

3.60. 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!

3.61. 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”.

3.62. 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

3.63. 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, $p = 3$).

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:

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

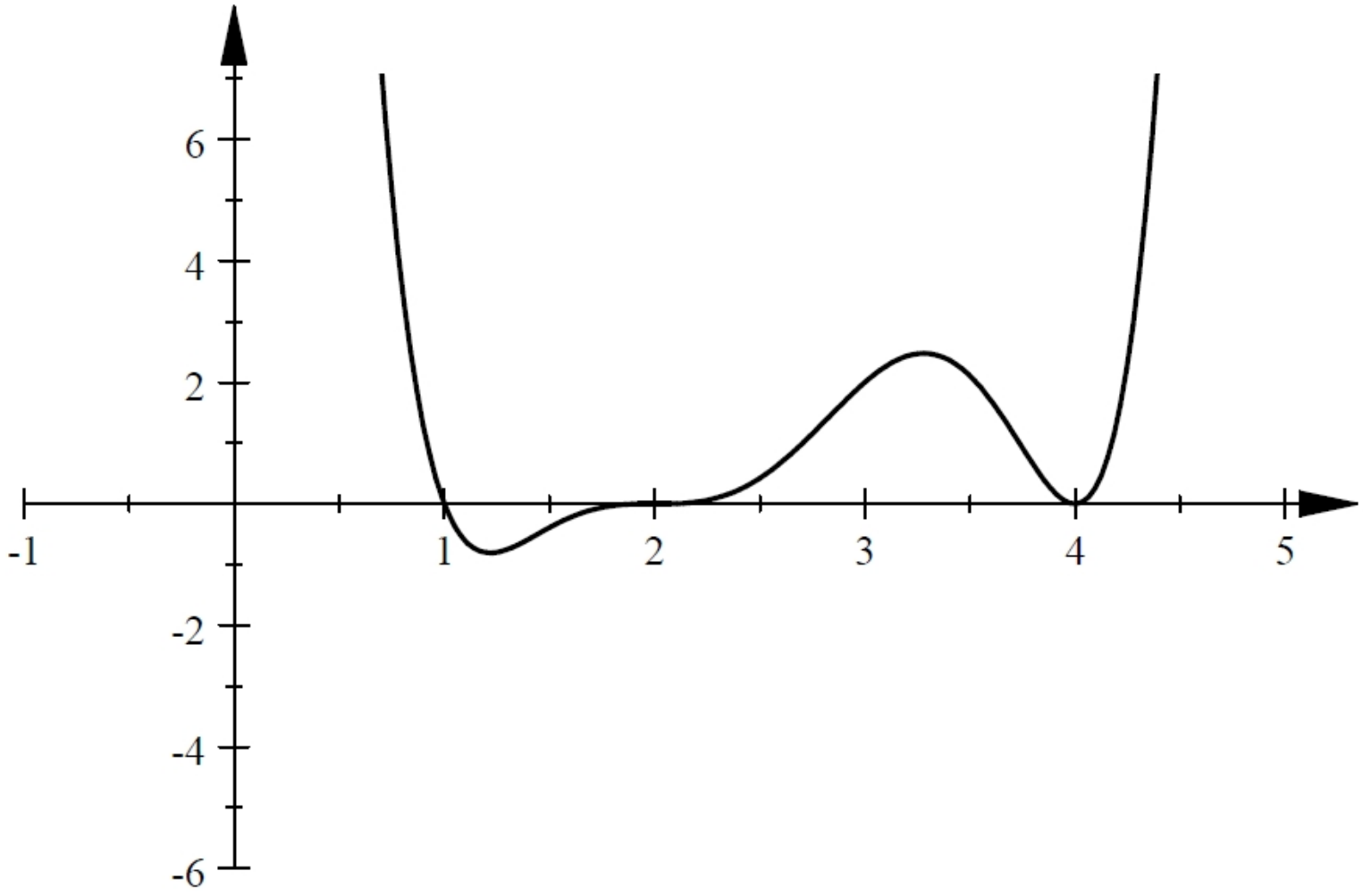
Mind a 32 esetben egyértelműen meg tudjuk határozni a g polinomot 
Lagrange-interpolációval.

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

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

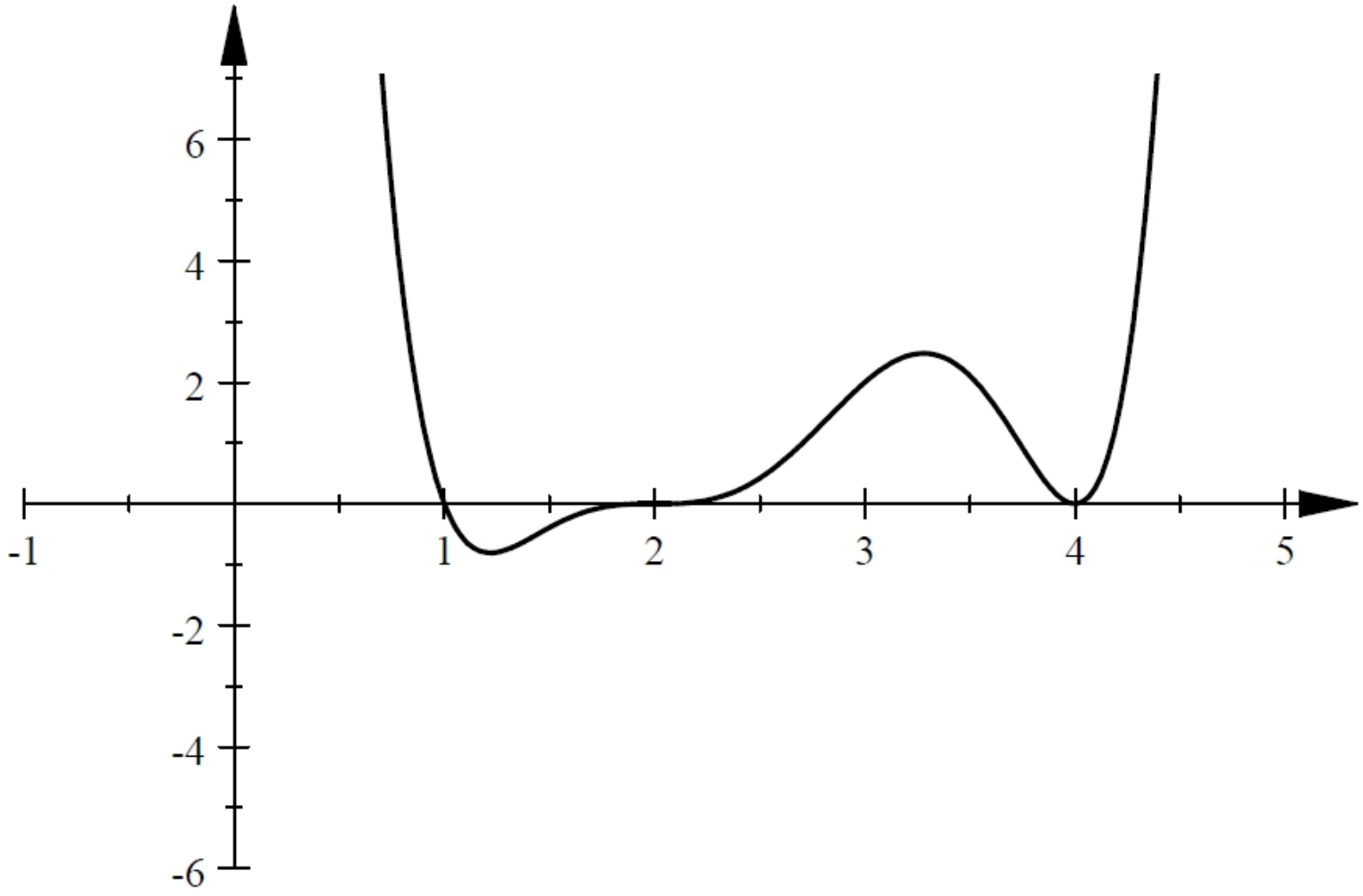
Valós polinomfüggvény deriváltja

$f = x^6 - 15x^5 + 90x^4 - 276x^3 + 456x^2 - 384x + 128$



Valós polinomfüggvény deriváltja

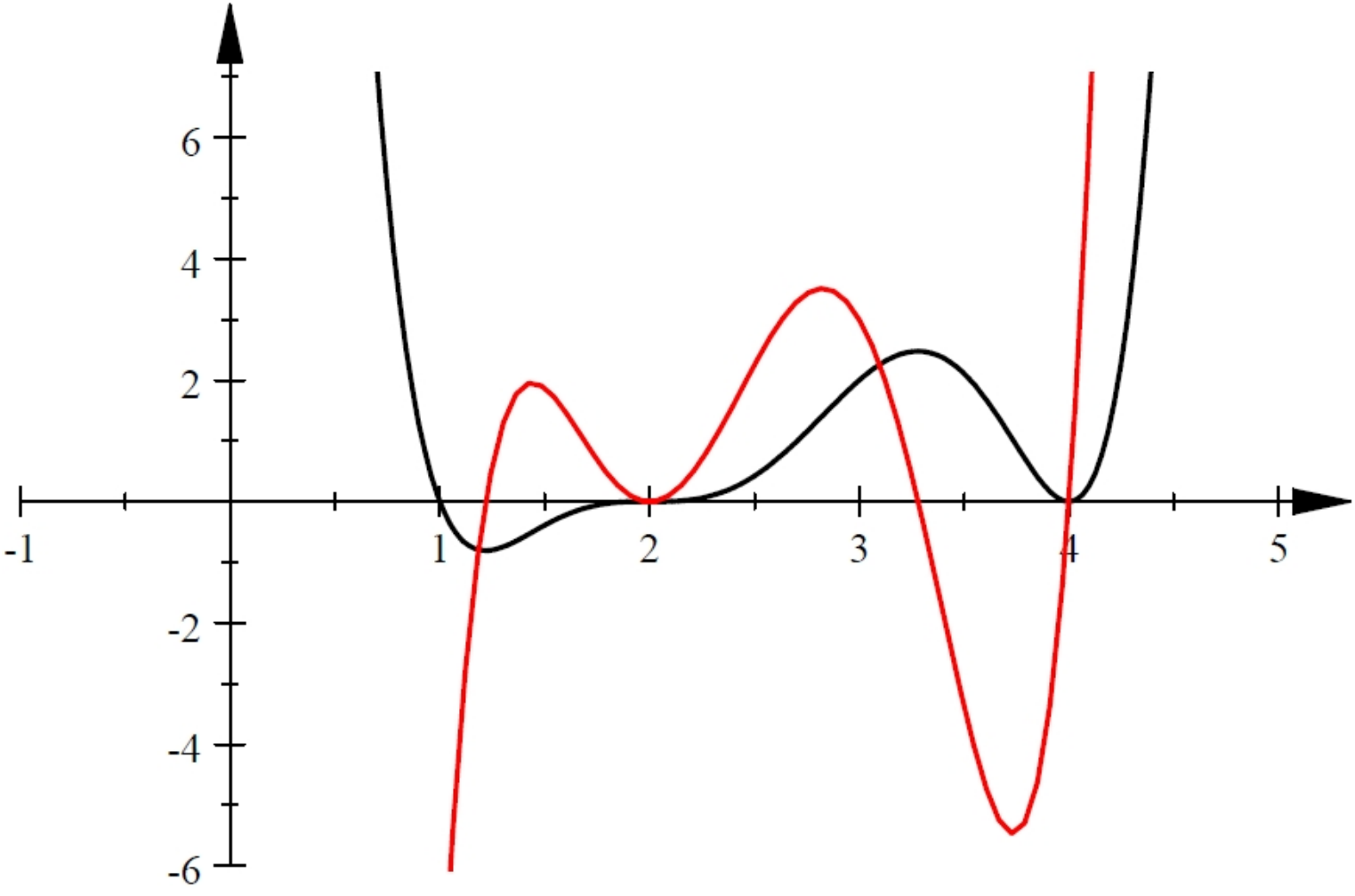
$$f = x^6 - 15x^5 + 90x^4 - 276x^3 + 456x^2 - 384x + 128 = (x-1)(x-2)^3(x-4)^2$$



Valós polinomfüggvény deriváltja

$f = x^6 - 15x^5 + 90x^4 - 276x^3 + 456x^2 - 384x + 128 = (x-1)(x-2)^3(x-4)^2$

$f' = 6x^5 - 75x^4 + 360x^3 - 828x^2 + 912x - 384$

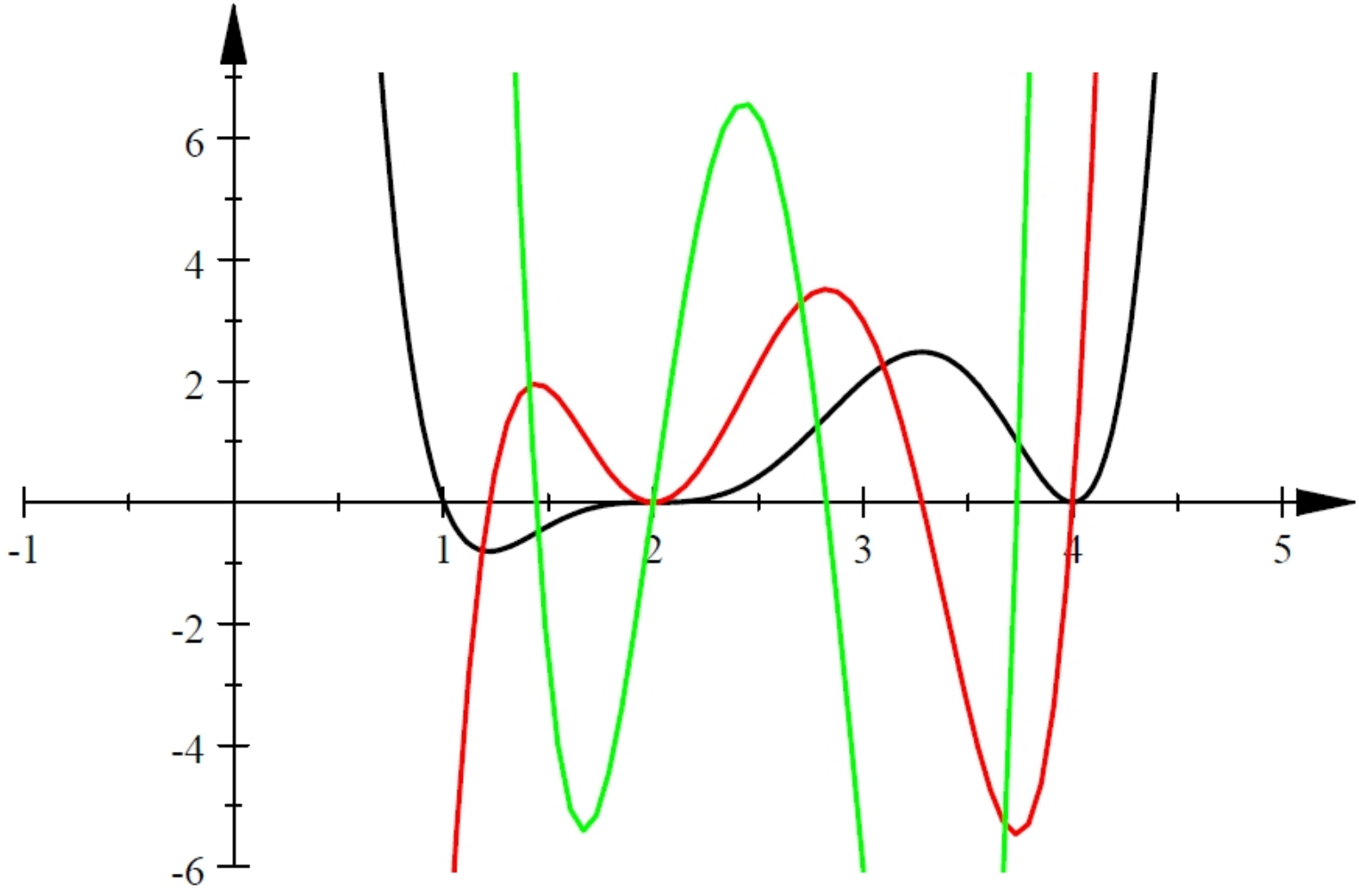


Valós polinomfüggvény deriváltja

$f = x^6 - 15x^5 + 90x^4 - 276x^3 + 456x^2 - 384x + 128 = (x-1)(x-2)^3(x-4)^2$

$f' = 6x^5 - 75x^4 + 360x^3 - 828x^2 + 912x - 384$

$f'' = 30x^4 - 300x^3 + 1080x^2 - 1656x + 912$



Polinom deriváltja

3.64. Definíció.

Az $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ polinom *deriváltj*án az

$$na_n x^{n-1} + \cdots + 2a_2 x + a_1$$

polinomot értjük.

Jelölés.

Az f polinom deriváltját f' jelöli, a k-adik deriváltat pedig $f^{(k)}$, az $f^{(1)} = f'$ és $f^{(0)} = f$ megállapodással.

3.65. Tétel.

Minden $f, g \in \mathbb{C}[x]$ polinomra és k pozitív egész számra érvényesek az alábbi deriválási szabályok:

(1) $(f+g)' = f' + g'$;

(2) $(fg)' = f'g + fg'$;

(3) $(f^k)' = kf^{k-1}f'$.

Polinom deriváltja

Bizonyítás.

A fenti definíció alapján „egyszerű” számolással ellenőrizhető (nem kell hozzá határérték!). Például, ha már (1) megvan, akkor (2)-ben elég *monomok*kal foglalkozni.

$$\begin{array}{lll} f = a\cdot x^k & g = b\cdot x^l & fg = ab\cdot x^{k+l} \\ f' = ka\cdot x^{k-1} & g' = lb\cdot x^{l-1} & (fg)' = (k+l)\,ab\cdot x^{k+l-1} \end{array}$$

Ezek alapján

$$\begin{aligned} f'g+fg' &= kax^{k-1}\cdot bx^l + ax^k\cdot lbx^{l-1} \\ &= kab\cdot x^{k-1+l} + lab\cdot x^{k+l-1} \\ &= (kab+lab)\cdot x^{k+l-1} \\ &= (k+l)\,ab\cdot x^{k+l-1}. \end{aligned}$$

□

Deriált és többszörös gyökök

3.66. Tétel.

Ha $k \geq 1$ és az α komplex szám k-szoros gyöke az f polinomnak, akkor $k-1$-szeres gyöke f'-nek. (Ha $k = 1$, akkor α nem gyöke f'-nek.)

Bizonyítás.

Ha az α gyök multiplicitása k, akkor

$$f = (x-\alpha)^k \cdot g, \text{ ahol } g(\alpha) \neq 0.$$

Deriváljunk!

$$\begin{aligned} f' &= k(x-\alpha)^{k-1} \cdot g + (x-\alpha)^k \cdot g' \\ &= (x-\alpha)^{k-1} \cdot (kg + (x-\alpha) g'). \end{aligned}$$

Tehát α  legalább $(k-1)$-szeres gyöke f'-nak. Hogy pontosan $(k-1)$-szeres gyöke legyen, ahhoz az kell, hogy  a kék polinomnak már ne legyen gyöke:

$$kg(\alpha) + (\alpha-\alpha) g'(\alpha) = kg(\alpha) \neq 0.$$

□

Derivált és többszörös gyökök

3.67. Megjegyzés.

Az előző tétel megfordítása nem igaz: f'-nek lehetnek olyan gyökei is, amelyekért nem f a „felelős”.

3.68. Következmény.

Az $f \in \mathbb{C}[x]$ polinom α gyökének multiplicitása nem más, mint a legkisebb olyan k nemnegatív egész, amelyre $f^{(k)}(\alpha) \neq 0$, azaz α akkor és csak akkor k-szoros gyök, ha $f(\alpha) = f'(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$, de $f^{(k)}(\alpha) \neq 0$.

Bizonyítás.

$$
\begin{array}{lllll}
 & \alpha & k\text{-szoros gyöke} & f\text{-nek} \\
\Longrightarrow & \alpha & (k-1)\text{-szeres gyöke} & f'\text{-nak} \\
\Longrightarrow & \alpha & (k-2)\text{-szörös gyöke} & f''\text{-nak} \\
\vdots & \vdots & \vdots & \vdots \\
\Longrightarrow & \alpha & 1\text{-szeres gyöke} & f^{(k-1)}\text{-nak} \\
\Longrightarrow & \alpha & 0\text{-szoros gyöke} & f^{(k)}\text{-nak.}
\end{array}
$$

□

Derivált és többszörös gyökök

3.69. Következmény.

Az α komplex szám akkor és csak akkor többszörös gyöke az $f \in \mathbb{C}[x]$ polinomnak, ha gyöke $\operatorname{lnko}(f, f')$*-nak.*

Bizonyítás.

$$\begin{aligned} \alpha \text{ többszörös gyöke } f\text{-nek} &\iff \alpha \text{ közös gyöke } f\text{-nek és } f'\text{-nak} \\ &\iff \alpha \text{ gyöke } \operatorname{lnko}(f, f')\text{-nak} \end{aligned}$$

□

3.70. Következmény.

Bármely legalább elsőfokú $f \in \mathbb{C}[x]$ polinomra az $\frac{f}{\operatorname{lnko}(f,f')}$ polinom gyökei ugyanazok, mint f gyökei, de mindegyik egyszeres gyök.

Bizonyítás.

Tfh. α egy k-szoros gyöke f-nek $(k \geq 1)$. Hányadik hatványon szerepel $(x - \alpha)$ ...?

$$\begin{aligned} & f && \text{felbontásában} && k\text{-adik hatványon} \\ \Longrightarrow\ & f' && \text{felbontásában} && (k-1)\text{-edik hatványon} \\ \Longrightarrow\ & \operatorname{lnko}(f, f') && \text{felbontásában} && (k-1)\text{-edik hatványon} \\ \Longrightarrow\ & f / \operatorname{lnko}(f, f') && \text{felbontásában} && \text{első hatványon.} \end{aligned}$$

□

Derivált és többszörös gyökök

Példa.

Határozzuk meg az $f = x^5 + x^4 - 5x^3 - x^2 + 8x - 4$ polinom gyökeit.

$$
\begin{aligned}
f' &= 5x^4 + 4x^3 - 15x^2 - 2x + 8 \\
\operatorname{lnko}(f, f') &= x^3 - 3x + 2 && \text{(euklideszi algoritmus)} \\
\frac{f}{\operatorname{lnko}(f,f')} &= x^2 + x - 2 = (x+2)(x-1) && \text{(maradékos osztás)} \\
f &= (x-1)^3 (x+2)^2 && \text{(Horner vagy deriválás)}
\end{aligned}
$$

Irreducibilis polinomnak nincs többszörös gyöke

3.71. Következmény.

Ha T számtest, azaz részteste $\mathbb{C}$-nek, és $f \in T[x]$ irreducibilis T felett, akkor f-nek minden komplex gyöke egyszeres.

Bizonyítás.

Mivel $\operatorname{lnko}(f, f') \in T[x]$  osztója f-nek és f irreducibilis, csak két lehetőség van:

1. $\operatorname{lnko}(f, f') \sim f$:  Ez nem lehet, mert  $\deg \operatorname{lnko}(f, f') \leq \deg f' < \deg f$.
2. $\operatorname{lnko}(f, f') \sim 1$:  Ekkor f-nek nincs többszörös gyöke.

□