Algebra és számelmélet előadás

Waldhauser Tamás
2016. október 27.

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

3.55. Tétel (Gauss-lemma).

Primitív polinomok szorzata is primitív.

Bizonyítás.

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

1. Létezik olyan $d > 1$ természetes szám, ami osztja az fg polinom minden együtthatóját. (Miért?)
2. Létezik olyan p prímszám, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$. (Miért?)
3. Erre a p prímre (sőt, igazából bármelyik p prímre) $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$ és $\overline{g} \neq \overline{0} \in \mathbb{Z}_p[x]$. (Miért?)
4. Ez pedig lehetetlen. (Miért?)

□

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

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 úgy, hogy egy egész együtthatós polinom akkor és csak akkor (ir)reducibilis $\mathbb{Z}$ felett, ha (ir)reducibilis $\mathbb{Q}$ 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).

Hetedik házi feladat az előadásra

Az alábbi linken megtalálható a 3.56. Tétel bizonyítása:

`https://www.overleaf.com/articles/eahf7/wgzcgkvdjdwt`

Indokolja meg a bizonyítás lépéseit: minden téglalapba írja be a bizonyítás valamelyik korábbi lépésének betűjelét és/vagy valamelyik előadásvázlat-beli tétel sorszámát, aszerint, hogy mit használunk az adott lépésnél.

- beküldendő emailben: `twaldha@math.u-szeged.hu`
- pdf fájl legyen (lehet szkennelt is)
- fájlnév: `EHA-eahf7.pdf` (például `WATHAAS-eahf7.pdf`)
- határidő: november 9, reggel 8 óra

Pontos oszthatóság

3.57. 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

3.58. 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.

3.59. 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.

3.60. 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”.

3.61. 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.

Bontsa $\mathbb{Q}$ 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.

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

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

A polinom irreducibilis $\mathbb{Q}$ felett: Schönemann-Eisenstein ($p = 2$).

Házi feladat a gyakorlatra

22. feladat. Határozza meg az alábbi polinomok irreducibilis felbontását $\mathbb{Q}$ felett.

(a) $2x^7 + 5x^6 + 4x^5 + 13x^4 + 54x^3 + 84x^2 + 54x + 12$

$(2x+1)(x+1)^2(x^4+6x+12)$

(b) $3x^{100} - 10x^{50} + 100x - 50$

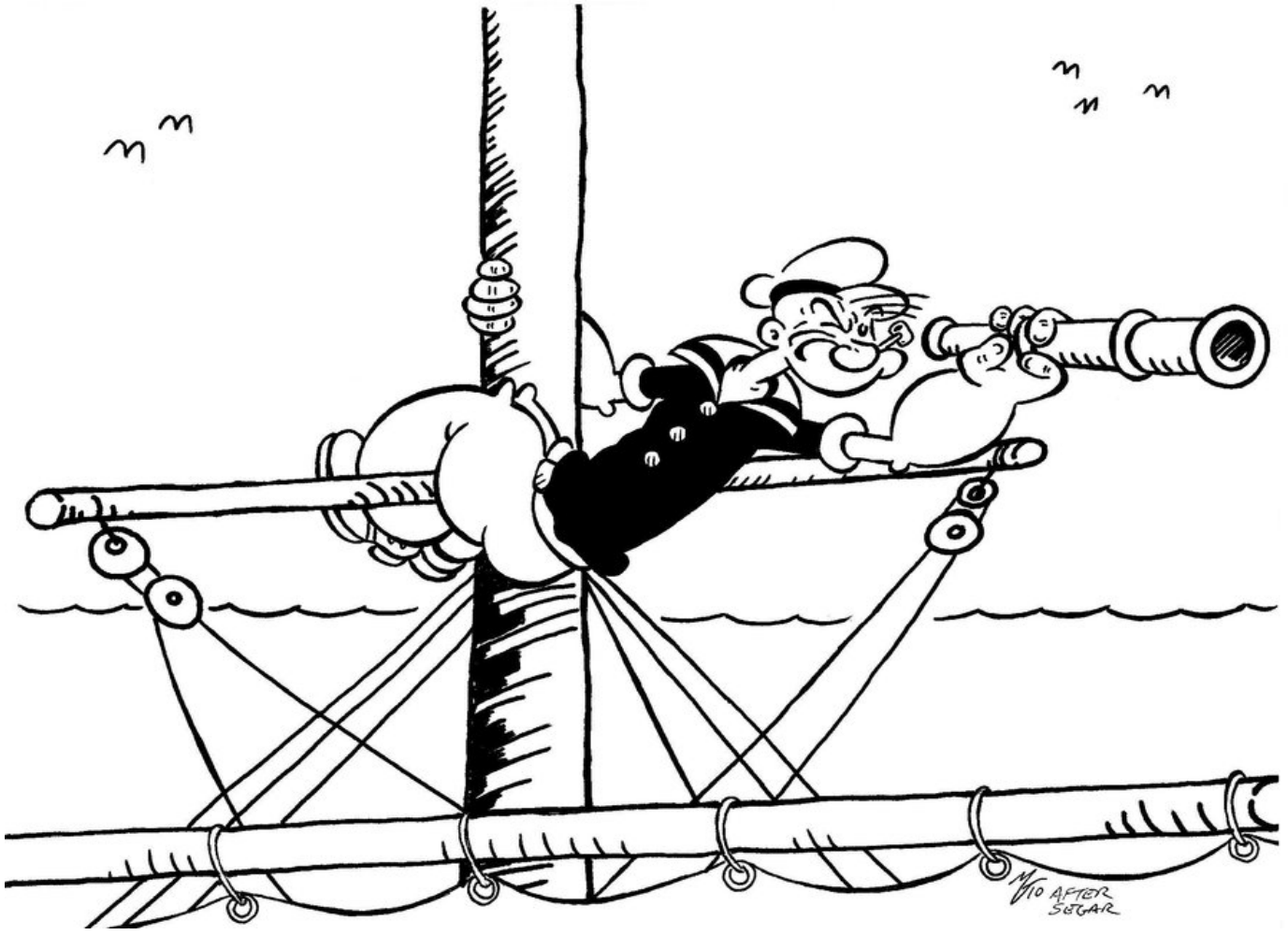
$3x^{100} - 10x^{50} + 100x - 50$

(c) $3x^6 + 2x^5 - 7x^4 + 2$

(d) $5x^8 - 5x^7 + 4x^2 - 2x - 2$

(e) $x^7 - 4x^6 + 4x^5 + 9x^4 - 36x^3 + 39x^2 - 12x + 12$

Kitekintés: további módszerek irreducibilitás vizsgálatára



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.

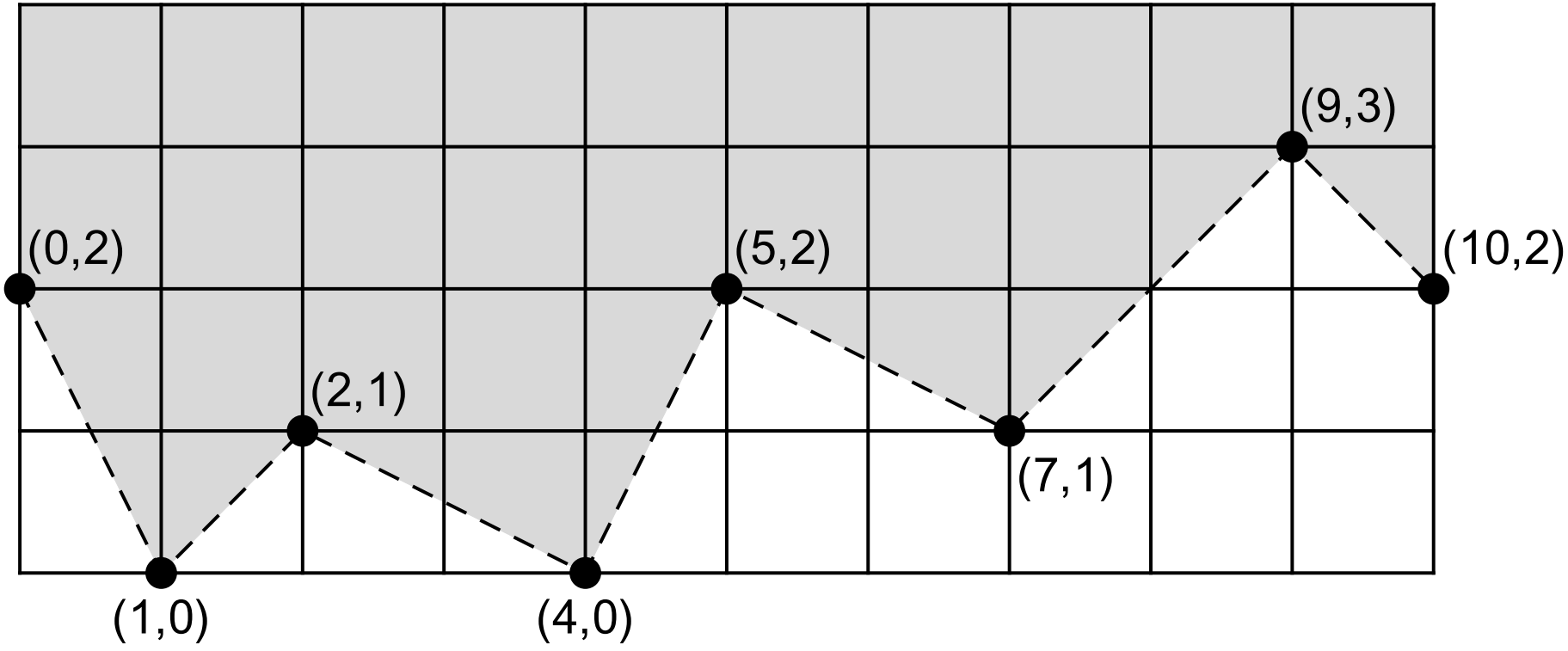
$$(a, b, c) = (1, 1, 3) \rightsquigarrow g = x^2 - x + 1 \rightsquigarrow f = (x^2 - x + 1)(x^2 - 3x + 3)$$

Newton-poligon

$f = 36 + 2x + 6x^2 + 2x^4 + 18x^5 + 3x^7 + 54x^9 + 18x^{10}$
$p = 3$

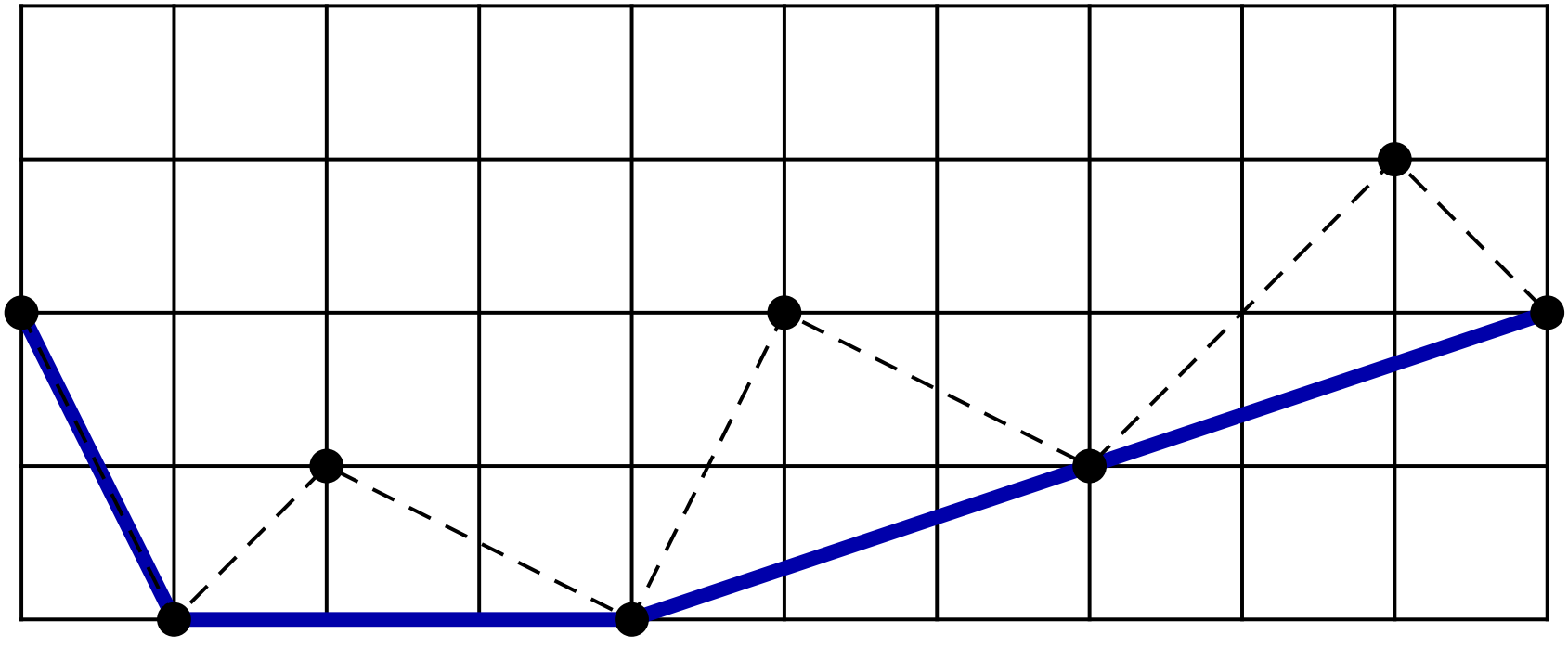
Newton-poligon

$f = 3^2 \cdot 4 + 3^0 \cdot 2x + 3^1 \cdot 2x^2 + 3^0 \cdot 2x^4 + 3^2 \cdot 2x^5 + 3^1 \cdot 1x^7 + 3^3 \cdot 2x^9 + 3^2 \cdot 2x^{10}$
$p = 3$



Newton-poligon

$f = 3^2 \cdot 4 + 3^0 \cdot 2x + 3^1 \cdot 2x^2 + 3^0 \cdot 2x^4 + 3^2 \cdot 2x^5 + 3^1 \cdot 1x^7 + 3^3 \cdot 2x^9 + 3^2 \cdot 2x^{10}$
$p = 3$



Dumas tétele

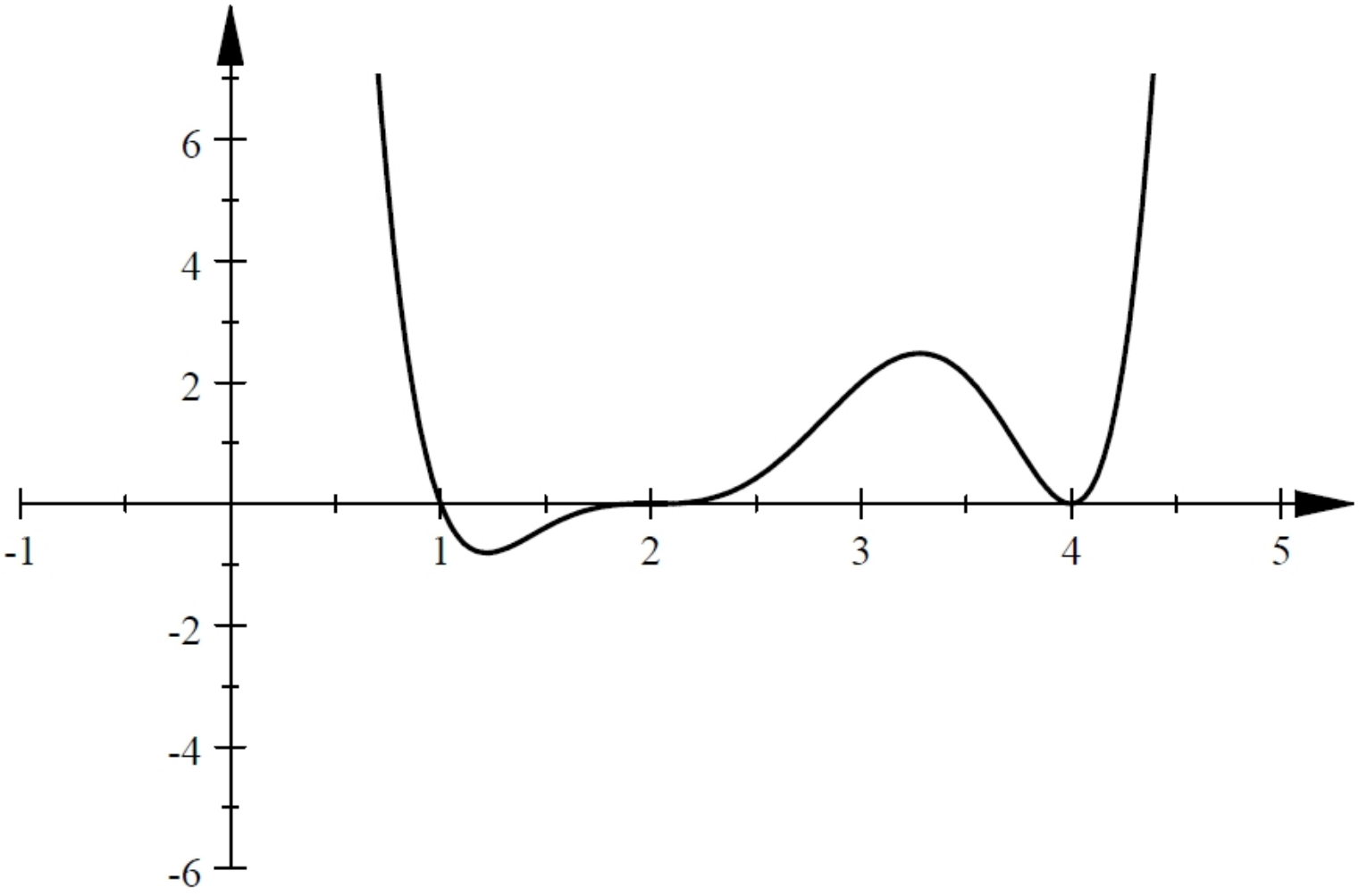
Tétel (Dumas, 1906).

Tetszőleges $f, g \in \mathbb{Z}[x]$ polinomok esetén $f \cdot g$ Newton-poligonja megkapható az f és g Newton-poligonját alkotó szakaszok összeillesztésével.

A bizonyítás elolvasható Sarró Mihály *Polinomok Newton-poligonjai* című szakdolgozatában (SZTE Bolyai Intézet, 2015).

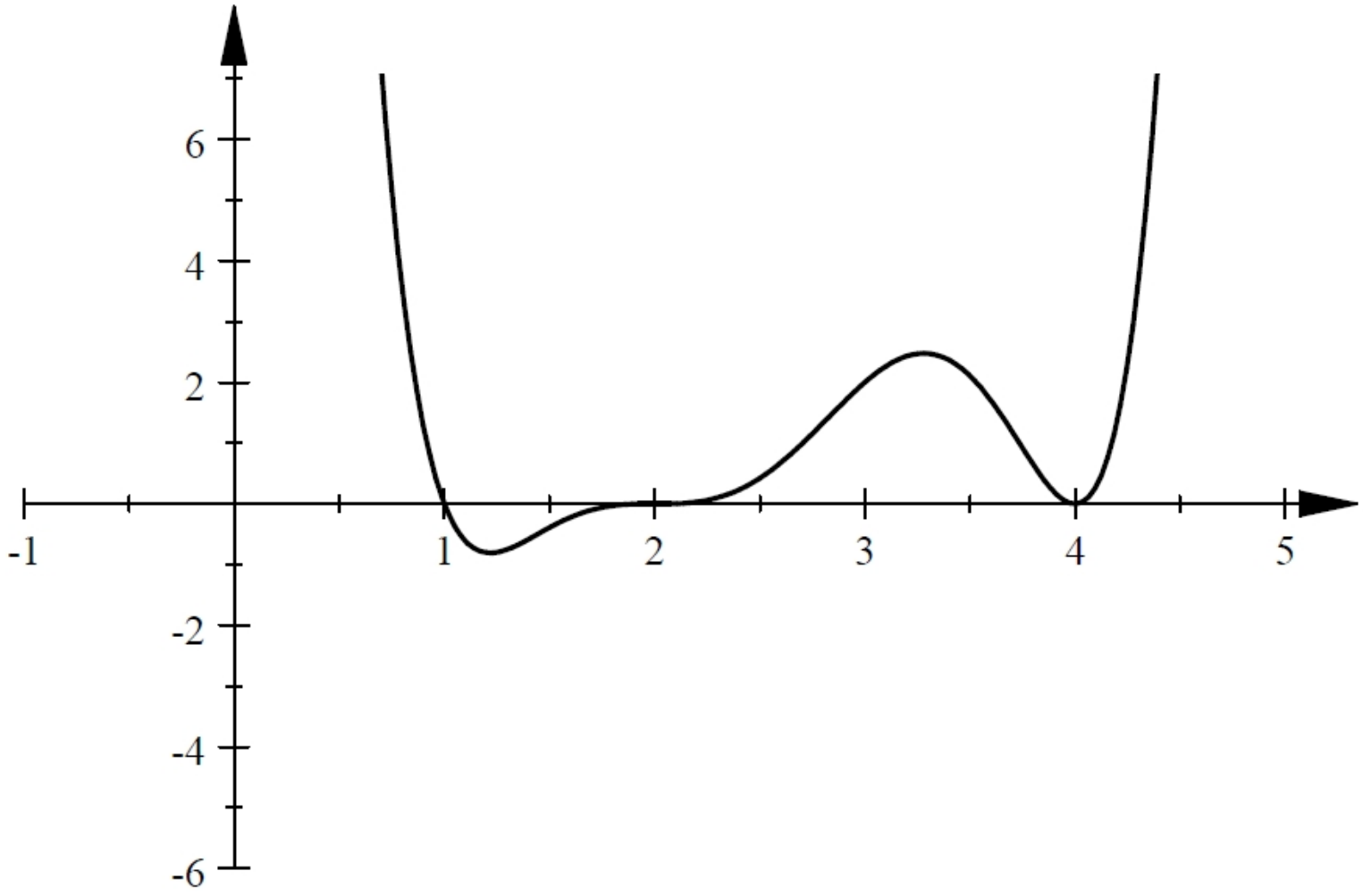
A Schönemann–Eisenstein-tétel triviális következménye a Dumas-tételnek: az ottani oszthatósági feltételek azt jelentik, hogy a Newton-poligon egyetlen szakaszból áll, így nem rakható össze kisebb darabokból.

Derivált, többszörös gyökök



Derivált, többszörös gyökök

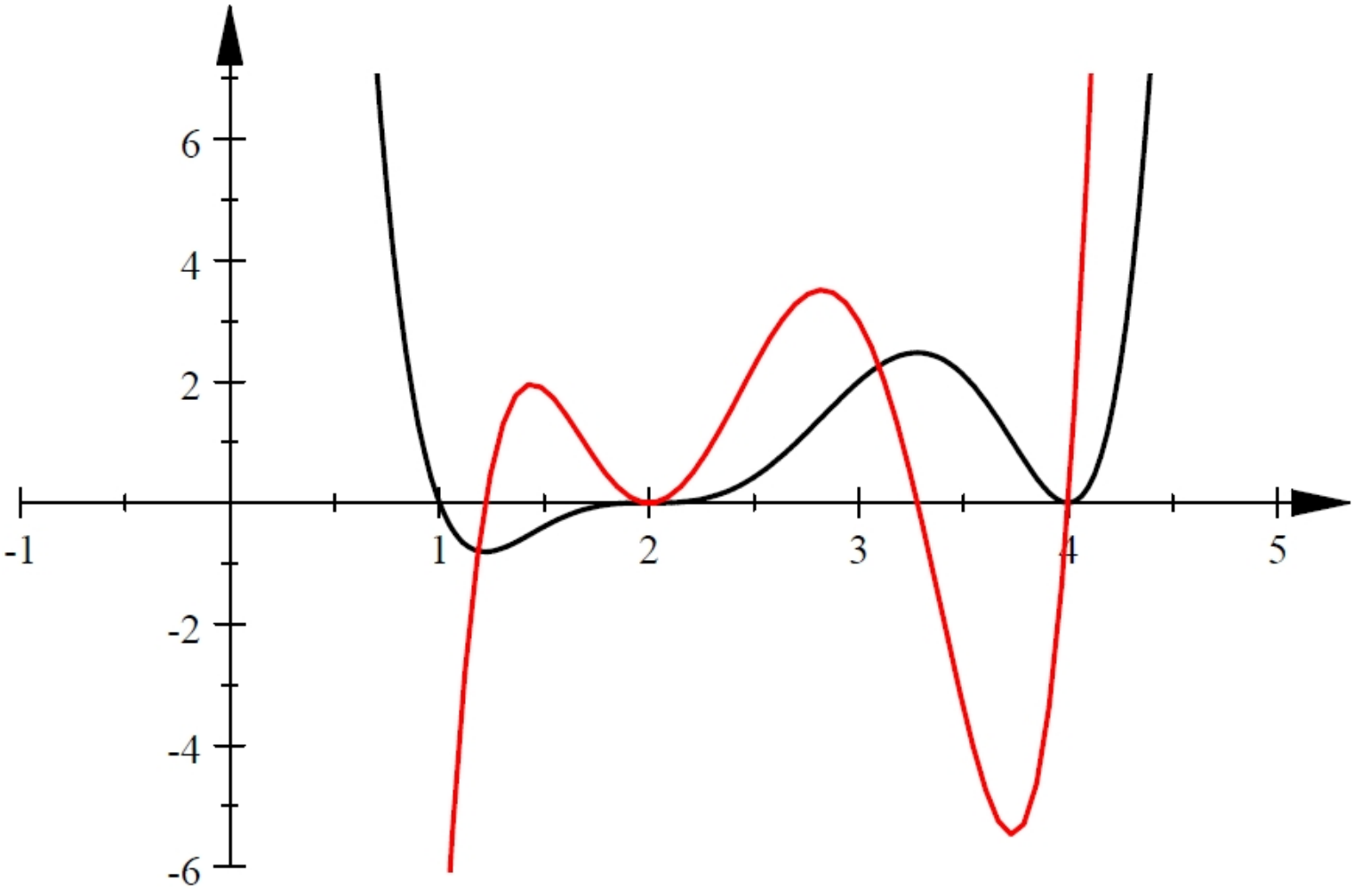
$$f = x^6 - 15x^5 + 90x^4 - 276x^3 + 456x^2 - 384x + 128 = (x-1)(x-2)^3(x-4)^2$$



Derivált, többszörös gyökök

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

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

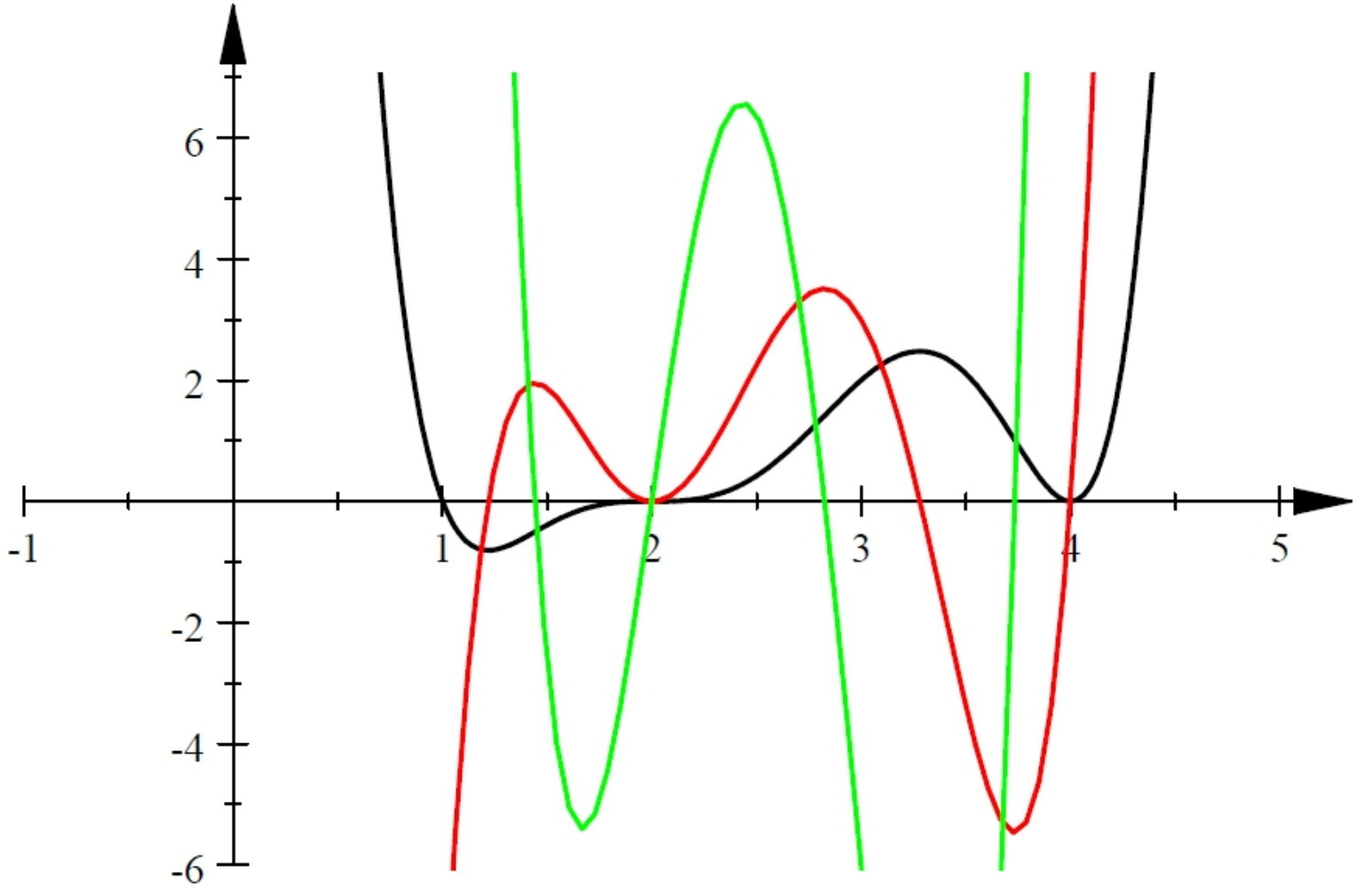


Derivált, többszörös gyökök

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

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

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



Polinom deriváltja

3.63. Definíció.

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

3.64. 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 *monomokkal* 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

3.65. 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

3.66. Megjegyzés.

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

3.67. 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

3.68. 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.

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

□

3.69. 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.

A derivált vizsgálatával határozza meg az alábbi f polinom többszörös gyökeit, majd az összes gyökét (multiplicitással együtt):

$$f = x^5 + x^4 - 5x^3 - x^2 + 8x - 4.$$

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

Házi feladat a gyakorlatra

23. feladat. A derivált vizsgálatával határozza meg az alábbi polinomok többszörös gyökeit, majd az összes gyököket (multiplicitással együtt). Az $\operatorname{lnko}(f, f')$ és $f / \operatorname{lnko}(f, f')$ polinomok kiszámításához használhat számítógépet.

(a) $x^5 + x^4 - 5x^3 - x^2 + 8x - 4$

$1, 1, 1, \ -2$

(b) $3x^4 - 4x^3 + 1$

$1, 1, \ \frac{-1 \pm \sqrt{2}i}{3}$

(c) $x^5 - 10x^3 - 20x^2 - 15x - 4$

(d) $x^7 - 3x^6 + 5x^5 - 7x^4 + 7x^3 - 5x^2 + 3x - 1$

(e) $x^6 - 15x^4 + 8x^3 + 51x^2 - 72x + 27$

Irreducibilis polinomnak nincs többszörös gyöke

3.70. 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.

□

Házi feladat a gyakorlatra

24. feladat. Döntse el, hogy igazak-e az alábbi állítások. A választ minden esetben indokolni kell!

(a) Ha egy legalább elsőfokú polinom irreducibilis, akkor nincsen gyöke.

nem, pl. x irreducibilis, mégis van gyöke

(b) Tetszőleges p prímszám esetén minden $f : \mathbb{Z}_p \to \mathbb{Z}_p$ leképezéshez létezik olyan $\mathbb{Z}_p[x]$-beli polinom, amelynek éppen f a polinomfüggvénye.

igen, pl. a $\left(\overline{0}, f\left(\overline{0}\right)\right), \ldots, \left(\overline{p-1}, f\left(\overline{p-1}\right)\right)$ pontokra illesztett Lagrange–féle interpolációs polinom

(c) Bármely $a, b, c \in \mathbb{R}$ számokra létezik olyan $f \in \mathbb{R}[x]$ másodfokú polinom, melyre $f(0) = a, f(1) = b$ és $f(2) = c$.

(d) Ha egy $\mathbb{C}$ feletti polinom irreducibilis, akkor van gyöke.

(e) Ha egy polinom relatív prím a deriváltjához, akkor nincsen többszörös gyöke.