# Diszkrét matematika II.
# 5. előadás

Fancsali Szabolcs Levente
nudniq@inf.elte.hu

ELTE IK Komputeralgebra Tanszék

Mérai László diái alapján

# Gyűrűk (múlt heti anyag!)

### Állítás

Legyen $(R; \oplus, \otimes)$ gyűrű $0 \in R$ nullelemmel. Ekkor $\forall r \in R$ esetén $0 \otimes r = r \otimes 0 = 0$.

### Bizonyítás

$0 \otimes r = (0 \oplus 0) \otimes r = (0 \otimes r) \oplus (0 \otimes r) \Longrightarrow 0 = 0 \otimes r$.
A másik állítás bizonyítása ugyanígy.

### Állítás

Test nullosztómentes.

### Bizonyítás

Legyen $(F; \oplus, \otimes)$ test $0 \in F$ nullelemmel, és $1 \in F$ egységelemmel.
Indirekt tfh. léteznek $a, b \in F$ nem-nulla elemek, amikre $a \otimes b = 0$.
Ekkor $b = 1 \otimes b = a^{-1} \otimes a \otimes b = a^{-1} \otimes 0 = 0$, ami ellentmondás.

# Polinomok alapfogalmai (múlt heti anyag!)

## Definíció

Legyen $(R;+,\cdot)$ gyűrű. A gyűrű elemeiből képzett $f=(f_0,f_1,f_2,\dots)$ $(f_j\in R)$ végtelen sorozatot $R$ fölötti polinomnak nevezzük, ha csak véges sok eleme nem-nulla.
Az $R$ fölötti polinomok halmazát $R[x]$-szel jelöljük.
$R[x]$ elemein definiáljuk az összeadást és a szorzást.
$f=(f_0,f_1,f_2,\dots)$, $g=(g_0,g_1,g_2,\dots)$ és $h=(h_0,h_1,h_2,\dots)$ esetén
$f+g=(f_0+g_0,f_1+g_1,f_2+g_2,\dots)$ és $f\cdot g=h$, ahol

$$h_k=\sum_{i+j=k}f_ig_j=\sum_{i=0}^{k}f_ig_{k-i}=\sum_{j=0}^{k}f_{k-j}g_j.$$

Két polinom pontosan akkor egyenlő, ha minden tagjuk egyenlő:

$$f=g\Leftrightarrow\forall j\in\mathbb{N}:f_j=g_j.$$

## Megjegyzés

Könnyen látható, hogy polinomok összege és szorzata is polinom.

# Polinomok alapfogalmai (múlt heti anyag!)

## Állítás (HF)

Ha $(R;+,\cdot)$ gyűrű, akkor $(R[x];+,\cdot)$ is gyűrű, és $R$ fölötti **polinomgyűrűnek** nevezzük.

## Megjegyzés

Gyakran az $(R;+,\cdot)$ gyűrűre szimplán $R$-ként, az $(R[x];+,\cdot)$ gyűrűre $R[x]$-ként hivatkozunk.

## Állítás

Ha az $R$ gyűrű kommutatív, akkor $R[x]$ is kommutatív.

## Bizonyítás

$$(f\cdot g)_k = f_0g_k + f_1g_{k-1} + \ldots + f_{k-1}g_1 + f_kg_0 =$$
$$= g_kf_0 + g_{k-1}f_1 + \ldots + g_1f_{k-1} + g_0f_k =$$
$$= g_0f_k + g_1f_{k-1} + \ldots + g_{k-1}f_1 + g_kf_0 = (g\cdot f)_k$$

# Polinomok alapfogalmai (múlt heti anyag!)

## Állítás

$1 \in R$ egységelem esetén $e = (1, 0, 0 \dots)$ egységeleme lesz $R[x]$-nek.

## Bizonyítás

$$(f \cdot e)_k = \sum_{j=0}^{k} f_j e_{k-j} = \sum_{j=0}^{k-1} f_j e_{k-j} + f_k e_0 = f_k$$

## Állítás

Ha az $R$ gyűrű nullosztómentes, akkor $R[x]$ is nullosztómentes.

## Bizonyítás

Legyen $n$, illetve $m$ a legkisebb olyan index, amire $f_n \neq 0$, illetve $g_m \neq 0$.

$$(f \cdot g)_{n+m} = \sum_{j=0}^{n+m} f_j g_{n+m-j} = \sum_{j=0}^{n-1} f_j g_{n+m-j} + f_n g_m + \sum_{j=n+1}^{n+m} f_j g_{n+m-j} =$$

$$= 0 + f_n g_m + 0 = f_n g_m \neq 0$$

# Polinomok alapfogalmai (múlt heti anyag!)

## Jelölés

Az $f = (f_0, f_1, f_2, \dots, f_n, 0, 0, \dots)$, $f_n \neq 0$ ($f_m = 0 : \forall m > n$) polinomot $f(x) = f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n$, $f_n \neq 0$ alakba írjuk.

## Definíció

Az előző pontban szereplő polinom esetén $f_i$-t az $i$-ed fokú tag együtthatójának nevezzük, $f_0$ a polinom konstans tagja, $f_n$ a főegyütthatója. A polinom tagjai az $f_j x^j$ alakú kifejezések, $f_n x^n$ a főtagja, $n$ pedig a foka. $f$ fokának jelölésére $deg(f)$ használatos.

## Példa

Az $f = (1, 0, 2, 0, 0, 3, 0, \dots)$ polinom felírható
$f(x) = 1 + 0x + 2x^2 + 0x^3 + 0x^4 + 3x^5$ alakban.
Ugyanezen $f$ további alakjai:
$f(x) = 1 + 2x^2 + 3x^5$, $f(x) = 3x^5 + 2x^2 + 1$.

# Polinomok alapfogalmai (ezzel kezdődik az új anyag)

## Megjegyzés

A főegyüttható tehát a legnagyobb indexű nem-nulla együttható, a fok pedig ennek indexe.
A $0 = (0, 0, \dots)$ nullpolinomnak nincs legnagyobb indexű nem-nulla együtthatója, így a fokát külön definiáljuk, mégpedig $deg(0) = -\infty$.

## Definíció

A konstans polinomok a legfeljebb nulladfokú polinomok, a lineáris polinomok pedig a legfeljebb elsőfokú polinomok. Az $f_i x^i$ alakba írható polinomok a monomok. Ha $f \in R[x]$ polinom főegyütthatója $R$ egységeleme, akkor $f$-et főpolinomnak nevezzük.

## Példa

- $x^3 + 1 \in \mathbb{Z}[x]$
- $\frac{2}{3} \in \mathbb{Q}[x]$
- $\pi x + (i + \sqrt{2}) \in \mathbb{C}[x]$

# Alapfogalmak

## Állítás

Legyen $f, g \in R[x]$, $deg(f) = n$, és $deg(g) = k$. Ekkor:

- $deg(f + g) \leq \max(n, k)$;
- $deg(f \cdot g) \leq n + k$.

## Bizonyítás

Legyen $h = f + g$. Ekkor $j > \max(n, k)$ esetén $h_j = 0 + 0 = 0$.
Legyen $h = f \cdot g$. Ekkor $j > n + k$ esetén

$$h_j = \sum_{i=0}^{j} f_i g_{j-i} = \sum_{i=0}^{n} f_i g_{j-i} + \sum_{i=n+1}^{j} f_i g_{j-i} = \sum_{i=0}^{n} f_i \cdot 0 + \sum_{i=n+1}^{j} 0 \cdot g_{j-i} = 0.$$

# Polinomok alapfogalmai

## Megjegyzés

Nullosztómentes gyűrű esetén egyenlőség teljesül a 2. egyenlőtlenségben, hiszen

$$h_{n+k} = \sum_{i=0}^{n+k} f_i g_{n+k-i} = \sum_{i=0}^{n-1} f_i g_{n+k-i} + f_n g_k + \sum_{i=n+1}^{n+k} f_i g_{n+k-i} = f_n g_k \neq 0.$$

# Polinomok alapfogalmai

## Definíció (helyettesítési érték)

Az $f(x) = f_0 + f_1x + f_2x^2 + \ldots + f_nx^n \in R[x]$ polinom $r \in R$ helyen felvett helyettesítési értékén az $f(r) = f_0 + f_1r + f_2r^2 + \ldots + f_nr^n \in R$ elemet értjük.

## Definíció (gyök)

$f(r) = 0$ esetén $r$-et a polinom gyökének nevezzük.

Példa $f(x) = x^2 + x - 2 \in \mathbb{Z}[x]$-nek a $-2$ helyen felvett helyettesítési értéke $(-2)^2 + (-2) - 2 = 0$, ezért $-2$ gyöke $f$-nek.

## Definíció (polinomfüggvény)

Az $\hat{f} : r \mapsto f(r)$ leképezés az $f$ polinomhoz tartozó polinomfüggvény.

Másik tárgyban lehet, hogy az itt "polinomfüggvénynek" nevezett cuccot hívtátok "polinomnak", és bizonyos esetekben ez nem is okoz gondot, de ebben a tárgyban gondosan ügyeljetek a két fogalom közötti különbségre!

# Polinomok alapfogalmai

## Megjegyzés

Ha $R$ véges, akkor csak véges sok $R \to R$ függvény van, míg végtelen sok $R[x]$-beli polinom, így vannak olyan polinomok, amikhez ugyanaz a polinomfüggvény tartozik, például $x, x^2 \in \mathbb{Z}_2[x]$.

## Megjegyzés

Ha $R$ végtelen elemszámú nullosztómentes gyűrű, akkor hiába van végtelen sok $R \to R$ függvény és végtelen sok $R[x]$-beli polinom, mégis lesznek olyan függvények, amik nem tartozhatnak egyetlen polinomhoz sem annak polinomfüggvényeként.

# Horner-elrendezés

Legyen $f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_1 x + f_0$, ahol $f_n \neq 0$. Ekkor átrendezéssel a következő alakot kapjuk:
$f(x) = (\cdots((f_n \cdot x + f_{n-1}) \cdot x + f_{n-2}) \cdot x + \ldots + f_1) \cdot x + f_0$, és így
$f(c) = (\ldots((f_n \cdot c + f_{n-1}) \cdot c + f_{n-2}) \cdot c + \ldots + f_1) \cdot c + f_0$.

Vagyis $f(c)$ kiszámítható $n$ db szorzás és $n$ db összeadás segítségével.

| | $f_n$ | $f_{n-1}$ | $f_{n-2}$ | $\ldots$ | $f_0$ | |
|---|---|---|---|---|---|---|
| $c$ | $\times$ | $c_1 = f_n$ | $c_2 = c_1 c + f_{n-1}$ | $\ldots$ | $c_n = c_{n-1}c + f_1$ | $f(c) = c_n c + f_0$ |

Általánosan: $c_k = c_{k-1}c + f_{n-k+1}$, ha $1 < k \leq n$.

Kicsit bőbeszédűbb (de kézzel írva követhetőbb) elrendezésben:

| | $f_n$ | $f_{n-1}$ | $f_{n-2}$ | $\ldots$ | $f_1$ | $f_0$ |
|---|---|---|---|---|---|---|
| $c$ | $\times$ | $c \cdot c_1$ | $c \cdot c_2$ | $\ldots$ | $c \cdot c_{n-1}$ | $c_n c$ |
| | $c_1 = f_n$ | $c_2 = c_1 c + f_{n-1}$ | $c_3 = c_2 c + f_1$ | $\ldots$ | $c_n = c_{n-1}c + f_1$ | $f(c) = c_n c + f_0$ |

# Horner-elrendezés

## Példa

Határozzuk meg az $f(x) = x^4 - 3x^3 + x + 6$ polinom $-2$ helyen vett helyettesítési értékét!

| | 1 | -3 | 0 | 1 | 6 | |
|---|---|---|---|---|---|---|
| -2 | × | 1 | -5 | 10 | -19 | 44 |

Ha az $f(c)$ helyettesítési érték nulla, azaz, ha a $c$ gyöke az $f$ polinomnak, akkor a Horner-elrendezés alsó sorában (a helyettesítési érték előtt) annak a $g$ polinomnak az együtthatói szerepelnek, amire $f(x) = (x - c) \cdot g(x)$.

## Példa

Az $f(x) = x^4 - 4x^3 + 6x^2 - 4x + 1$ polinom $c = 1$ helyen vett helyettesítési értéke nulla:

| | 1 | -4 | 6 | -4 | 1 | |
|---|---|---|---|---|---|---|
| 1 | × | 1 | -3 | 3 | -1 | 0 |

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

# A maradékos osztás tétele és következményei

## Tétel (polinomok maradékos osztása)

Legyen $R$ egységelemes integritási tartomány, $f, g \in R[x]$, és tegyük fel, hogy $g$ főegyütthatója egység $R$-ben. Ekkor egyértelműen léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = qg + r$, ahol $deg(r) < deg(g)$.

A fenti tétel az $f$ polinomnak a $g$ polinommal való maradékos elosztásának az egyértelmű elvégezhetőségét mondja ki.
A $q$ polinomot a maradékos osztás hányadospolinomjának, az $r$ polinomot az osztási maradékpolinomnak nevezzük.

# A maradékos osztás tétele és következményei

## Tétel (polinomok maradékos osztása)

Legyen $R$ egységelemes integritási tartomány, $f, g \in R[x]$, és tegyük fel, hogy $g$ főegyütthatója egység $R$-ben. Ekkor egyértelműen léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = qg + r$, ahol $deg(r) < deg(g)$.

## Bizonyítás

Létezés: $f$ foka szerinti TI: ha $deg(f) < deg(g)$, akkor $q = 0$ és $r = f$ esetén megfelelő előállítást kapunk.
Legyen $f$ főegyütthatója $f_n$, $g$ főegyütthatója $g_k$. $n \geq k$ esetén legyen $f^*(x) = f(x) - f_n g_k^{-1} g(x) x^{n-k}$.
$deg(f^*) < deg(f)$ (Miért?) miatt $f^*$-ra használhatjuk az indukciós feltevést, vagyis léteznek $q^*, r^* \in R[x]$ polinomok, amikre $f^* = q^* g + r^*$.
$f(x) = f^*(x) + f_n g_k^{-1} g(x) x^{n-k} = q^*(x) g(x) + r^*(x) + f_n g_k^{-1} g(x) x^{n-k} =$
így $q(x) = q^*(x) + f_n g_k^{-1} x^{n-k}$ és $r(x) = r^*(x)$ jó választás.

# A maradékos osztás tétele és következményei

## Bizonyítás folyt.

Egyértelműség: Tekintsük $f$ két megfelelő előállítását:
$f = qg + r = q^*g + r^*$, amiből:

$$g(q - q^*) = r^* - r.$$

Ha a bal oldal nem $0$, akkor a foka legalább $k$, de a jobb oldal foka legfeljebb $k - 1$, $0 = g(q - q^*) = r^* - r$, és így
$q = q^*$ és $r = r^*$.

# A maradékos osztás tétele és következményei

## Definíció

Ha $c \in R$ az $f \in R[x]$ polinom gyöke, akkor $(x - c) \in R[x]$ a $c$-hez tartozó gyöktényező.

## Következmény (gyöktényező leválasztása)

Legyen $R$ egységelemes integritási tartomány. Ha $0 \neq f \in R[x]$, és $c \in R$ gyöke $f$-nek, akkor létezik olyan $q \in R[x]$, amire $f(x) = (x - c)q(x)$.

## Bizonyítás

Osszuk el maradékosan $f$-et $(x - c)$-vel (Miért lehet?):

$$f(x) = q(x)(x - c) + r(x).$$

Mivel $deg(r(x)) < deg(x - c) = 1$, ezért $r$ konstans polinom.
Helyettesítsünk be $c$-t, így azt kapjuk, hogy
$0 = f(c) = q(c)(c - c) + r(c) = r(c)$,
amiből $r = 0$.

# A maradékos osztás tétele és következményei

## Következmény

Az $R$ egységelemes integritási tartomány fölötti $f \neq 0$ polinomnak legfeljebb $deg(f)$ gyöke van.

## Bizonyítás

$f$ foka szerinti TI:
$deg(f) = 0$-ra igaz az állítás (Miért?).
Ha $deg(f) > 0$, és $f(c) = 0$, akkor $f(x) = (x - c)g(x)$ (Miért?), ahol $deg(g) + 1 = deg(f)$ (Miért?). Ha $d$ gyöke $f$-nek, akkor $0 = f(d) = (d - c)g(d)$ azaz (Miért is?) vagy $d - c = 0$ (amiből $d = c$), vagy $g(d) = 0$ (azaz $d$ gyöke $g$-nek). Innen következik az állítás.

Ha $R$ gyűrű NEM egységelemes integritási tartomány (például azért, mert vannak benne nullosztók), akkor nem igaz a fenti állítás.
Például $\mathbb{Z}_6$ fölött:

$$(x - 2)(x - 3) \equiv x^2 + x \equiv (x - 0)(x + 1) \pmod{6}$$

# A maradékos osztás tétele és következményei

## Következmény

Ha $R$ egységelemes integritási tartomány, akkor ha két, legfeljebb $n$-ed fokú $R[x]$-beli polinomnak $n+1$ különböző helyen ugyanaz a helyettesítési értéke, akkor egyenlőek.

## Bizonyítás

A két polinom különbsége legfeljebb $n$-ed fokú, és $n+1$ gyöke van (Miért?), ezért nullpolinom (Miért?), vagyis a polinomok egyenlőek.

## Következmény

Ha $R$ végtelen egységelemes integritási tartomány, akkor két különböző $R[x]$-beli polinomhoz nem tartozik ugyanaz a polinomfüggvény.

## Bizonyítás

Ellenkező esetben a polinomok különbségének végtelen sok gyöke lenne (Miért?).

# Bővített euklideszi algoritmus

## Definíció

Azt mondjuk, hogy $f, g \in R[x]$ polinomok esetén $f$ osztója $g$-nek ($g$ többszöröse $f$-nek), ha létezik $h \in R[x]$, amire $g = f \cdot h$.

## Definíció

Az $f, g \in R[x]$ polinomok kitüntetett közös osztója (legnagyobb közös osztója) az a $d \in R[x]$ polinom, amelyre $d|f$, $d|g$, és tetszőleges $c \in R[x]$ esetén $(c|f \wedge c|g) \Rightarrow c|d$.

Test fölötti polinomgyűrűben tetszőleges nem-nulla polinommal tudunk maradékosan osztani, ezért működik a bővített euklideszi-algoritmus. Ez $f, g \in R[x]$ esetén ($R$ test) meghatározza $f$ és $g$ kitüntetett közös osztóját, a $d \in R[x]$ polinomot, továbbá $u, v \in R[x]$ polinomokat, amelyekre $d = u \cdot f + v \cdot g$.

# Bővített euklideszi algoritmus

## Algoritmus

Legyen $R$ test, $f, g \in R[x]$. Ha $g = 0$, akkor $(f, g) = f = 1 \cdot f + 0 \cdot g$, különben végezzük el a következő maradékos osztásokat:

$$
\begin{aligned}
f &= q_1 g + r_1;\\
g &= q_2 r_1 + r_2;\\
r_1 &= q_3 r_2 + r_3;\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n;\\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}
$$

Ekkor $d = r_n$ jó lesz kitüntetett közös osztónak.
Az $u_{-1} = 1,\ u_0 = 0,\ v_{-1} = 0,\ v_0 = 1$ kezdőértékekkel, továbbá az $u_k = u_{k-2} - q_k \cdot u_{k-1}$ és $v_k = v_{k-2} - q_k \cdot v_{k-1}$ rekurziókkal megkapható $u = u_n$ és $v = v_n$ polinomok olyanok, amelyekre teljesül $d = u \cdot f + v \cdot g$.

# Bővített euklideszi algoritmus

## Bizonyítás

A maradékok foka természetes számok szigorúan monoton csökkenő sorozata, ezért az eljárás véges sok lépésben véget ér.
Indukcióval belátjuk, hogy $r_{-1} = f$ és $r_0 = g$ jelöléssel $r_k = u_k \cdot f + v_k \cdot g$ teljesül minden $-1 \leq k \leq n$ esetén:
$k = -1$-re $f = 1 \cdot f + 0 \cdot g$, $k = 0$-ra $g = 0 \cdot f + 1 \cdot g$.
Mivel $r_{k+1} = r_{k-1} - q_{k+1} \cdot r_k$, így az indukciós feltevést használva:
$r_{k+1} = u_{k-1} \cdot f + v_{k-1} \cdot g - q_{k+1} \cdot (u_k \cdot f + v_k \cdot g) =$
$= (u_{k-1} - q_{k+1} \cdot u_k) \cdot f + (v_{k-1} - q_{k+1} \cdot v_k) \cdot g = u_{k+1} \cdot f + v_{k+1} \cdot g$.
Tehát $r_n = u_n \cdot f + v_n \cdot g$, és így $f$ és $g$ közös osztói $r_n$-nek is osztói.
Kell még, hogy $r_n$ osztója $f$-nek és $g$-nek.
Indukcióval belátjuk, hogy $r_n | r_{n-k}$ teljesül minden $0 \leq k \leq n+1$ esetén:
$k = 0$-ra $r_n | r_n$ nyilvánvaló, $k = 1$-re $r_{n-1} = q_{n+1} r_n$ miatt $r_n | r_{n-1}$.
$r_{n-(k+1)} = q_{n-(k-1)} r_{n-k} + r_{n-(k-1)}$ miatt az indukciós feltevést használva kapjuk az állítást, és így $k = n$, illetve $k = n+1$ helyettesítéssel $r_n | r_0 = g$, illetve $r_n | r_{-1} = f$.

# Polinomok algebrai deriváltja

## Definíció

Legyen $R$ gyűrű. Az
$f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_2 x^2 + f_1 x + f_0 \in R[x]$ $(f_n \neq 0)$ polinom
algebrai deriváltja az
$f'(x) = nf_n x^{n-1} + (n-1)f_{n-1}x^{n-2} + \ldots + 2f_2 x + f_1 \in R[x]$ polinom.

## Megjegyzés

Itt $kf_k = \underbrace{f_k + f_k + \ldots + f_k}_{k \text{ db}}$. (Ez akkor kell, ha $k \in \mathbb{N}^+$, de $k \notin R$.)

## Állítás

Legyen $R$ gyűrű, $a, b \in R$ és $n \in \mathbb{N}^+$. Ekkor $(na)b = n(ab) = a(nb)$.

## Bizonyítás

$$(\underbrace{a + a + \ldots + a}_{n \text{ db}})b = (\underbrace{ab + ab + \ldots + ab}_{n \text{ db}}) = a(\underbrace{b + b + \ldots + b}_{n \text{ db}})$$

# Polinomok algebrai deriváltja

## Állítás

Ha $R$ egységelemes integritási tartomány, akkor az $f \mapsto f'$ algebrai deriválás rendelkezik a következő tulajdonságokkal:

1. konstans polinom deriváltja a nullpolinom;
2. az $x$ polinom deriváltja az egységelem;
3. $(f+g)' = f' + g'$, ha $f, g \in R[x]$ (additivitás);
4. $(fg)' = f'g + fg'$, ha $f, g \in R[x]$ (szorzat differenciálási szabálya).

## Megjegyzés

Megfordítva, ha egy $R$ egységelemes integritási tartomány esetén egy $f \mapsto f'$, $R[x]$-et önmagába képező leképzés rendelkezik az előző 4 tulajdonsággal, akkor az az algebrai deriválás.

# Polinomok algebrai deriváltja

## Állítás

Ha $R$ egységelemes integritási tartomány, $c \in R$ és $n \in \mathbb{N}^+$, akkor $((x-c)^n)' = n(x-c)^{n-1}$.

## Bizonyítás

$n$ szerinti TI:
$n = 1$ esetén $(x-c)' = 1 = 1 \cdot (x-c)^0$.
Tfh. $n = k$-ra teljesül az állítás, vagyis $((x-c)^k)' = k(x-c)^{k-1}$.
Ekkor
$$((x-c)^{k+1})' = ((x-c)^k(x-c))' = ((x-c)^k)'(x-c) + (x-c)^k(x-c)' =$$
$$= k(x-c)^{k-1}(x-c) + (x-c)^k \cdot 1 = (k+1)(x-c)^k.$$
Ezzel az állítást beláttuk.

## Állítás (NB)

Ha $R$ integritási tartomány, $char(R) = p$, és $0 \neq r \in R$, akkor $n \cdot r = 0 \iff p|n$.

# Polinomok algebrai deriváltja

## Definíció

Legyen $R$ egységelemes integritási tartomány, $0 \neq f \in R[x]$ és $n \in \mathbb{N}^+$. Azt mondjuk, hogy $c \in R$ az $f$ egy $n$-szeres gyöke, ha $(x-c)^n | f$, de $(x-c)^{n+1} \not| f$. Ekkor $c$ multiplicitása $n$.

## Megjegyzés

A definíció azzal ekvivalens, hogy $f(x) = (x-c)^n g(x)$, ahol $c$ nem gyöke $g$-nek. (Miért?)

## Tétel

Legyen $R$ egységelemes integritási tartomány, $f \in R[x]$, $n \in \mathbb{N}^+$ és $c \in R$ az $f$ egy $n$-szeres gyöke. Ekkor $c$ az $f'$-nek legalább $(n-1)$-szeres gyöke, és ha $char(R) \not| n$, akkor pontosan $(n-1)$-szeres gyöke.

# Polinomok algebrai deriváltja

## Bizonyítás

Ha $f(x) = (x-c)^n g(x)$, ahol $c$ nem gyöke $g$-nek, akkor
$f'(x) = ((x-c)^n)' g(x) + (x-c)^n g'(x) =$
$= n(x-c)^{n-1} g(x) + (x-c)^n g'(x) = (x-c)^{n-1}(ng(x) + (x-c)g'(x))$.
Tehát $c$ tényleg legalább $(n-1)$-szeres gyöke $f'$-nek, és akkor lesz $(n-1)$-szeres gyöke, ha c nem gyöke $ng(x) + (x-c)g'(x)$-nek, vagyis $0 \neq ng(c) + (c-c)g'(c) = ng(c) + 0 \cdot g'(c) = ng(c)$. Ez pedig teljesül, ha $char(R) \not| n$.

## Példa

Legyen $f(x) = x^4 - x \in \mathbb{Z}_3[x]$. Ekkor $1$ 3-szoros gyöke $f$-nek, mert

$$f(x) = x(x^3-1) \overset{\mathbb{Z}_3}{=} x(x^3 - 3x^2 + 3x - 1) = x(x-1)^3.$$

$$f'(x) = 4x^3 - 1 \overset{\mathbb{Z}_3}{=} x^3 - 3x^2 + 3x - 1 = (x-1)^3,$$

tehát $1$ 3-szoros gyöke $f'$-nek is.

# Lagrange-interpoláció

## Tétel

Legyen $R$ test, $c_0, c_1, \ldots, c_n \in R$ különbözőek, továbbá $d_0, d_1, \ldots, d_n \in R$ tetszőlegesek. Ekkor létezik egy olyan legfeljebb $n$-ed fokú polinom, amelyre $f(c_j) = d_j$, ha $j = 0, 1, \ldots, n$.

## Bizonyítás

Legyen

$$\ell_j(x) = \frac{\prod_{i \neq j}(x - c_i)}{\prod_{i \neq j}(c_j - c_i)},$$

a $j$-edik Lagrange-interpolációs alappolinom, és legyen

$$f(x) = \sum_{j=0}^{n} d_j \ell_j(x).$$

$\ell_j(c_i) = 0$, ha $i \neq j$, és $\ell_j(c_j) = 1$-ből következik az állítás.

# Lagrange-interpoláció

## Példa

Adjunk meg olyan $f \in \mathbb{R}[x]$ polinomot, amelyre $f(0) = 3$, $f(1) = 3$, $f(4) = 7$ és $f(-1) = 0$!

A feladat szövege alapján $c_0 = 0$, $c_1 = 1$, $c_2 = 4$, $c_3 = -1$, $d_0 = 3$, $d_1 = 3$, $d_2 = 7$ és $d_3 = 0$ értékekkel alkalmazzuk a Lagrange-interpolációt.

$\ell_0(x) = \frac{(x-1)(x-4)(x+1)}{(0-1)(0-4)(0+1)} = \frac{1}{4}x^3 - x^2 - \frac{1}{4}x + 1$

$\ell_1(x) = \frac{(x-0)(x-4)(x+1)}{(1-0)(1-4)(1+1)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 + \frac{2}{3}x$

$\ell_2(x) = \frac{(x-0)(x-1)(x+1)}{(4-0)(4-1)(4+1)} = \frac{1}{60}x^3 - \frac{1}{60}x$

$\ell_3(x) = \frac{(x-0)(x-1)(x-4)}{(-1-0)(-1-1)(-1-4)} = -\frac{1}{10}x^3 + \frac{1}{2}x^2 - \frac{2}{5}x$

$f(x) = 3\ell_0(x) + 3\ell_1(x) + 7\ell_2(x) + 0\ell_3(x) = \frac{22}{60}x^3 - \frac{3}{2}x^2 + \frac{68}{60}x + 3$

| | $\frac{22}{60}$ | $-\frac{3}{2}$ | $\frac{68}{60}$ | $3$ | |
|---|---|---|---|---|---|
| $1$ | $\times$ | $\frac{22}{60}$ | $-\frac{68}{60}$ | $0$ | $3$ |
| $4$ | $\times$ | $\frac{22}{60}$ | $-\frac{2}{60}$ | $1$ | $7$ |
| $-1$ | $\times$ | $\frac{22}{60}$ | $-\frac{112}{60}$ | $3$ | $0$ |

# Lagrange-interpoláció

## Alkalmazás

A Lagrange-interpoláció használható titokmegosztásra a következő módon:
legyenek $1 \leq m < n$ egészek, továbbá $s \in \mathbb{N}$ a titok, amit $n$ ember között akarunk szétosztani úgy, hogy bármely $m$ részből a titok rekonstruálható legyen, de kevesebből nem. Válasszunk a titok maximális lehetséges értékénél és $n$-nél is nagyobb $p$ prímet, továbbá $a_1, a_2, \ldots, a_{m-1} \in \mathbb{Z}_p$ véletlen együtthatókat, majd határozzuk meg az $f(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1x + s$ polinomra az $f(i)$ értékeket, és adjuk ezt meg az $i$. embernek $(i = 1, 2, \ldots, n)$.
Bármely $m$ helyettesítési értékből a Lagrange-interpolációval megkapható a polinom, így annak konstans tagja is, a titok.
Ha $m$-nél kevesebb helyettesítési értékünk van, akkor nem tudjuk meghatározni a titkot, mert tetszőleges $t$ esetén az $f(0) = t$ értéket hozzávéve a többihez létezik olyan legfeljebb $m$-ed fokú polinom, aminek a konstans tagja $t$, és az adott helyeken megfelelő a helyettesítési értéke.

# Titokmegosztás

## Példa

Legyen $m = 3$, $n = 4$, $s = 5$, $p = 7$, továbbá $a_1 = 3$ és $a_2 = 4$. Ekkor $f(x) = 4x^2 + 3x + 5 \in \mathbb{Z}_7[x]$, a titokrészletek pedig $f(1) = 5$, $f(2) = 6$, $f(3) = 1$ és $f(4) = 4$. Ha rendelkezünk például az $f(1) = 5$, $f(3) = 1$ és $f(4) = 4$ információkkal, akkor $c_0 = 1$, $c_1 = 3$, $c_2 = 4$, $d_0 = 5$, $d_1 = 1$, és $d_2 = 4$ értékekkel alkalmazzuk a Lagrange-interpolációt.

$$\ell_0(x) = \frac{(x-3)(x-4)}{(1-3)(1-4)} = \frac{1}{6}(x^2 - 7x + 12) = \frac{1}{-1}(-6x^2 - 2) = 6x^2 + 2$$

$$\ell_1(x) = \frac{(x-1)(x-4)}{(3-1)(3-4)} = -\frac{1}{2}(x^2 - 5x + 4) = -4(x^2 + 2x + 4) = 3x^2 + 6x + 5$$

$$\ell_2(x) = \frac{(x-1)(x-3)}{(4-1)(4-3)} = \frac{1}{3}(x^2 - 4x + 3) = 5(x^2 + 3x + 3) = 5x^2 + x + 1$$

$$f(x) = 5\ell_0(x) + \ell_1(x) + 4\ell_2(x) = 30x^2 + 10 + 3x^2 + 6x + 5 + 20x^2 + 4x + 4 =$$
$$= 53x^2 + 10x + 19 = 4x^2 + 3x + 5$$