# Diszkrét matematika 2. C szakirány

5-6. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2016. tavasz

# Gyűrűk

## Definíció

Legyen $(R; *, \circ)$ algebrai struktúra, ahol $*$ és $\circ$ binér műveletek. Azt mondjuk, hogy teljesül a $\circ$-nek a $*$-ra vonatkozó bal oldali disztributivitása, illetve jobb oldali disztributivitása, ha
$\forall k, l, m \in R$-re: $k \circ (l * m) = (k \circ l) * (k \circ m)$, illetve
$\forall k, l, m \in R$-re: $(l * m) \circ k = (l \circ k) * (m \circ k)$.

## Példa

$(\mathbb{Z}; +, \cdot)$ esetén teljesül a szorzás összeadásra vonatkozó mindkét oldali disztributivitása.

## Elnevezés

$(R; *, \circ)$ két binér műveletes algebrai struktúra esetén a $*$-ra vonatkozó semleges elemet nullelemnek, a $\circ$-re vonatkozó semleges elemet egységelemnek nevezzük. A nullelem szokásos jelölése $0$, az egységelemé $1$, esetleg $e$.

# Gyűrűk

## Definíció

Az $(R; *, \circ)$ két binér műveletes algebrai struktúra gyűrű, ha

- $(R; *)$ Abel-csoport;
- $(R; \circ)$ félcsoport;
- teljesül a $\circ$-nek a $*$-ra vonatkozó mindkét oldali disztributivitása.

Az $(R; *, \circ)$ gyűrű egységelemes gyűrű, ha $R$-en a $\circ$ műveletre nézve van egységelem.
Az $(R; *, \circ)$ gyűrű kommutatív gyűrű, ha a $\circ$ művelet (is) kommutatív.

## Példa

- $(\mathbb{Z}; +, \cdot)$ egységelemes kommutatív gyűrű.
- $(2\mathbb{Z}; +, \cdot)$ gyűrű, de nem egységelemes.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ a szokásos műveletekkel egységelemes kommutatív gyűrűk.
- $\mathbb{C}^{k \times k}$ a szokásos műveletekkel egységelemes gyűrű, de nem kommutatív, ha $k > 1$.

# Nullosztómentes gyűrűk

## Definíció

Ha egy $(R, *, \circ)$ gyűrűben $\forall r, s \in R$, $r, s \neq 0$ esetén $r \circ s \neq 0$, akkor $R$ nullosztómentes gyűrű.

## Példa

Nem nullosztómentes gyűrű

- $(\mathbb{R}^{2\times 2}; +, \cdot)$: $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

## Állítás

Nullosztómentes gyűrűben a nem-nulla elemek additív rendje megegyezik, és vagy egy $p$ prímszám vagy végtelen.

## Definíció

Ha az előző állításban szereplő közös rend $p$, akkor a gyűrű karakterisztikája $p$, ha a közös rend végtelen, akkor pedig $0$. Jelölése: $char(R)$.

# Nullosztómentes gyűrűk

## Definíció

A kommutatív, nullosztómentes gyűrűt integritási tartománynak nevezzük.

## Példa

- $(\mathbb{Z}; +, \cdot)$

## Definíció

Az $(R; *, \circ)$ egységelemes integritási tartományban az $a, b \in R$ elemekre azt mondjuk, hogy $a$ osztója $b$-nek, ha van olyan $c \in R$, amire $b = a \circ c$.
Jelölése: $a|b$.

## Definíció

Az egységelem osztóját egységnek nevezzük.

# Testek

## Definíció

Az $(R; *, \circ)$ gyűrű **ferdetest**, ha $(R \setminus \{0\}; \circ)$ csoport. A kommutatív ferdetestet **testnek** nevezzük.

## Példa

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a szokásos műveletekkel,
- $\mathbb{Z}_p$ a szokásos műveletekkel, ha $p$ prím.

# Alapfogalmak

## 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

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

## Megjegyzés

Könnyen látható, hogy polinomok összege és szorzata is polinom.

# Alapfogalmak

### Állítás (NB)

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.

### Állítás

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

# Alapfogalmak

## 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 $g_m \neq 0$.

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

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

# Alapfogalmak

## Jelölés

Az $f = (f_0, f_1, f_2, \ldots, f_n, 0, 0, \ldots)$, $f_n \neq 0$ polinomot $f(x) = f_0 + f_1x + f_2x^2 + \ldots + f_nx^n$, $f_n \neq 0$ 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**, $f_nx^n$ a **főtagja**, $n$ pedig a **foka**. $f$ fokának jelölésére $deg(f)$ használatos.

# Alapfogalmak

## 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

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

# Alapfogalmak

## Megjegyzés

Nullosztómentes gyűrű esetén egyenlőség teljesül a 2. egyenlőtlenségben, hiszen

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

# Alapfogalmak

## Definíció

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.

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

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

## 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 $x, x^2 \in \mathbb{Z}_2[x]$.

## 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.

# 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 $1 < k \leq n$.

## Példa

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

| | 1 | -3 | 0 | 1 | 6 | |
|---|---|---|---|---|---|---|
| -2 | $\times$ | 1 | -5 | 10 | -19 | 44 |

# 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 $f^* = q^* g + r^*$.
$f(x) = f^*(x) + f_n g_k^{-1} g(x) x^{n-k} = q^*(x) g(x) + r^*(x) + f_n g_k^{-1} g(x) x^{n-k} =$
$= (q^*(x) + f_n g_k^{-1} x^{n-k}) g(x) + r^*(x)$,
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 $k - 1$, tehát
$0 = g(q - q^*) = r^* - r$, és így
$q = q^*$ és $r = r^*$.

## Definíció

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

# A maradékos osztás tétele és következményei

## Következmény (gyöktényező leválasztása)

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 $f \neq 0$ 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 $d - c = 0$, amiből $d = c$, vagy $d$ gyöke $g$-nek (Miért?). Innen következik az állítás.

# A maradékos osztás tétele és következményei

### Következmény

Ha két, legfeljebb $n$-ed fokú 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, 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 $kf_k = \underbrace{f_k + f_k + \ldots + f_k}_{k \text{ db}}$.

## 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
$$((x-c)^{k+1})' = ((x-c)^k(x-c))' = ((x-c)^k)'(x-c) + (x-c)^k(x-c)' =$$
$$= k(x-c)^{k-1}(x-c) + (x-c)^k \cdot 1 = (x-c)^k(k+1).$$
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 $(x-c)^{n+1} \nmid f$.

## 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 $char(R) \nmid n$, 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

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

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

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

$l_j(c_i) = 0$, ha $i \neq j$, és $l_j(c_j) = 1$-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.

$$l_0(x) = \frac{(x-1)(x-4)(x+1)}{(0-1)(0-4)(0+1)} = \frac{1}{4}x^3 - x^2 - \frac{1}{4}x + 1$$

$$l_1(x) = \frac{(x-0)(x-4)(x+1)}{(1-0)(1-4)(1+1)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 + \frac{2}{3}x$$

$$l_2(x) = \frac{(x-0)(x-1)(x+1)}{(4-0)(4-1)(4+1)} = \frac{1}{60}x^3 - \frac{1}{60}x$$

$$l_3(x) = \frac{(x-0)(x-1)(x-4)}{(-1-0)(-1-1)(-1-4)} = -\frac{1}{10}x^3 + \frac{1}{2}x^2 - \frac{2}{5}x$$

$$f(x) = 3l_0(x) + 3l_1(x) + 7l_2(x) + 0l_3(x) = \frac{22}{60}x^3 - \frac{3}{2}x^2 + \frac{68}{60}x + 3$$

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

# Polinomok felbonthatósága

## Definíció

Legyen $R$ egységelemes integritási tartomány.
Ha a $0 \neq f \in R[x]$ polinom nem egység, akkor felbonthatatlannak (irreducibilisnek) nevezzük, ha $\forall a, b \in R[x]$-re

$$f = a \cdot b \Longrightarrow (a \text{ egység} \vee b \text{ egység}) .$$

Ha a $0 \neq f \in R[x]$ polinom nem egység, és nem felbonthatatlan, akkor felbonthatónak (reducibilisnek) nevezzük.

## Megjegyzés

Utóbbi azt jelenti, hogy $f$-nek van nemtriviális szorzat-előállítása (olyan, amiben egyik tényező sem egység).

# Polinomok felbonthatósága

## Állítás

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

## Állítás

Test nullosztómentes.

## Állítás

Legyen $(F; +, \cdot)$ test. Ekkor $f \in F[x]$ pontosan akkor egység, ha $deg(f) = 0$.

## Bizonyítás

Később.

# Polinomok felbonthatósága

## Állítás

Legyen $(F;+,\cdot)$ test, és $f \in F[x]$. Ha $deg(f) = 1$, akkor $f$-nek van gyöke.

## Bizonyítás

Később.

## Megjegyzés

Ha $(R;+,\cdot)$ nem test, akkor egy $R$ fölötti elsőfokú polinomnak nem feltétlenül van gyöke, pl. $2x - 1 \in \mathbb{Z}[x]$.

# Polinomok felbonthatósága

## Állítás

Legyen $(F;+,\cdot)$ test, és $f \in F[x]$. Ha $deg(f) = 1$, akkor $f$ felbonthatatlan.

## Bizonyítás

Később.

## Megjegyzés

Tehát nem igaz, hogy egy felbonthatatlan polinomnak nem lehet gyöke.

# Polinomok felbonthatósága

## Állítás

Legyen $(F;+,\cdot)$ test, és $f \in F[x]$. Ha $2 \leq deg(f) \leq 3$, akkor $f$ pontosan akkor felbontható, ha van gyöke.

## Bizonyítás

Később.

# Polinomok felbonthatósága

## Tétel

$f \in \mathbb{C}[x]$ pontosan akkor felbonthatatlan, ha $deg(f) = 1$.

## Bizonyítás

Később.

## Tétel

$f \in \mathbb{R}[x]$ pontosan akkor felbonthatatlan, ha

- $deg(f) = 1$, vagy
- $deg(f) = 2$, és $f$-nek nincs (valós) gyöke.

## Bizonyítás

Később.

# Polinomok felbonthatósága

## Definíció

$f \in \mathbb{Z}[x]$-et primitív polinomnak nevezzük, ha az együtthatóinak a legnagyobb közös osztója $1$.

## Tétel (Schönemann-Eisenstein)

Legyen $f(x) = f_n x^n + f_{n-1}x^{n-1} + \ldots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ legalább elsőfokú primitív polinom. Ha található olyan $p \in \mathbb{Z}$ prím, melyre

- $p \not| f_n$,
- $p | f_j$, ha $0 \leq j < n$,
- $p^2 \not| f_0$,

akkor $f$ felbonthatatlan $\mathbb{Z}$ fölött.

## Bizonyítás

NB. (Lehet, hogy később igen.)

# Polinomok felbonthatósága

## Megjegyzés

A feltételben $f_n$ és $f_0$ szerepe felcserélhető.

## Megjegyzés

A tétel nem használható test fölötti polinom irreducibilitásának bizonyítására, mert testben nem léteznek prímek, hiszen minden nem-nulla elem egység.