# Diszkrét matematika II.
# 4. előadás

Fancsali Szabolcs Levente
nudniq@inf.elte.hu

ELTE IK Komputeralgebra Tanszék

Mérai László diái alapján

# Műveletek (múlt heti anyag!)

## Definíció (Művelet)

Egy $X$ halmazon értelmezett ($r$-változós, "$r$-ér") művelet alatt egy $* : X^r \to X$ függvényt értünk.
Egy $X$ halmazon értelmezett binér (kétváltozós) művelet egy $* : X \times X \to X$ függvény. Gyakran $*(x, y)$ helyett $x * y$-t írunk.
Egy $X$ halmazon értelmezett unér (egyváltozós) művelet egy $* : X \to X$ függvény.

## Példa

- $\mathbb{C}$ halmazon az $+$ is, és $\cdot$ is binér műveletek.
- $\mathbb{C}$ halmazon az $\div$ (osztás) nem művelet, mert $\mathrm{dmn}(\div) \neq \mathbb{C} \times \mathbb{C}$.
- $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ halmazon az $\div$ binér művelet.
- $\mathbb{C}$ halmazon a $0$ illetve $1$ konstans kijelölése nullér művelet.
- $\mathbb{R}^n$ ($n > 1$) vektortéren a vektorok skaláris szorzása nem művelet, mert $\mathrm{rng}(\langle , \rangle) = \mathbb{R} \neq \mathbb{R}^n$ (a szorzás eredménye nem vektor)
- $\mathbb{R}^n$ vektortéren egy adott $\lambda \in \mathbb{R}$ skalárral való szorzás unér művelet

# Műveleti tulajdonságok (múlt heti anyag!)

## Definíció

A $* : X \times X \to X$ művelet:
- asszociatív, ha $\forall a, b, c \in X : (a * b) * c = a * (b * c)$;
- kommutatív, ha $\forall a, b \in X : a * b = b * a$.

## Példa

- $\mathbb{C}$-n az $+$ ill. a $\cdot$ műveletek asszociatívak, kommutatívak.
- A függvények halmazán a kompozíció művelete asszociatív: $(f \circ g) \circ h = f \circ (g \circ h)$.
- A függvények halmazán a kompozíció művelete nem kommutatív: $f(x) = x + 1$, $g(x) = x^2$: $x^2 + 1 = (f \circ g)(x) \neq (g \circ f)(x) = (x + 1)^2$.
- A kivonás az egész számok halmazán nem asszociatív: $-1 = (1 - 1) - 1 \neq 1 - (1 - 1) = 1$.

# Művelettartó leképezések (múlt heti anyag!)

## Definíció

Legyen $X$ halmaz a $*$ művelettel, $Y$ a $\circ$ művelettel. Az $f : X \to Y$ függvény művelettartó, ha $\forall x, y \in X$ esetén

$$f(x * y) = f(x) \circ f(y).$$

## Példa

- Legyen $X = \mathbb{R}$ az $+$ művelettel, $Y = \mathbb{R}^+$ a $\cdot$ művelettel. Ekkor az $x \mapsto a^x$ művelettartó: $a^{x+y} = a^x \cdot a^y$.
- Legyen $X = Y = \mathbb{C}$ az $+$ művelettel. Ekkor a $z \mapsto \overline{z}$ művelettartó: $\overline{z + w} = \overline{z} + \overline{w}$.
- Legyen $X = \mathbb{Z}$ a $+$ művelettel, $Y = \mathbb{Z}_m$ a $+_m$ (összeadás modulo $m$) művelettel. Ekkor a $n \mapsto n \bmod m$ művelettartó: $(k + n) \bmod m = (k \bmod m) +_m (n \bmod m)$.
- Legyen $X = \{\mathrm{I}, \mathrm{H}\}$ a XOR/$\wedge$ művelettel, $\mathbb{Z}_2$ a $+/\cdot$ művelettel. Ekkor a $\mathrm{H} \mapsto 0$, $\mathrm{I} \mapsto 1$ hozzárendelés művelettartó (XOR-nak $+$).

# Algebrai struktúrák (múlt heti anyag!)

## Definíció (Algebrai struktúra)

A $(H; M)$ pár algebrai struktúra, ha $H$ egy halmaz, $M$ pedig $H$-n értelmezett műveletek halmaza.

A $(H; \{*, +, \circ\})$ jelölés helyett a $(H; *, +, \circ)$ jelölést is használhatjuk.

## Definíció (Grupoid)

Ha az $M$ művelethalmaz egyetlen műveletet tartalmaz, és az egy binér művelet, akkor a $(H; M)$ struktúrát grupoidnak nevezzük.

- $(\mathbb{N}; +)$ algebrai struktúra, mert természetes számok összege természetes szám (ld. Diszkrét matematika 1.), és grupoid is.
- $(\mathbb{N}; -)$ nem algebrai struktúra, mert például $0 - 1 = -1 \notin \mathbb{N}$.
- $(\mathbb{Z}; +, \cdot)$ algebrai struktúra, mert egész számok összege és szorzata egész szám (ld. Diszkrét matematika 1.), de nem grupoid.
- $(\mathbb{Z}_m; +, \cdot)$ algebrai struktúra (ld. Diszkrét matematika 1.), de nem grupoid, mert két művelet van.

# Félcsoportok (múlt heti anyag!)

## Definíció (Félcsoport)

A $(G; *)$ grupoid félcsoport, ha $*$ asszociatív $G$-n.

## Definíció (egységelem, semleges elem)

Ha létezik olyan $s \in G$ elem, amire $\forall g \in G : s * g = g * s = g$, akkor az $s$ elemet semleges elemnek (más néven egységelemnek) nevezzük.

## Definíció (Monoid)

Ha $(G; *)$ félcsoportban létezik $s$ semleges elem, akkor $G$-t semleges elemes félcsoportnak, egységelemes félcsoportnak, más néven monoidnak nevezzük.

- $\mathbb{N}$ az $+$ művelettel egységelemes félcsoport $n = 0$ egységelemmel.
- $\mathbb{Q}$ a $\cdot$ művelettel egységelemes félcsoport $n = 1$ egységelemmel.
- $\mathbb{C}^{k \times k}$ a mátrixszorzással egységelemes félcsoport az egységmátrixszal mint egységelemmel.

# Csoportok (itt kezdődik az új anyag)

## Definíció (elem inverze)

Legyen $(G; *)$ egy egységelemes félcsoport $e$ egységelemmel. A $g \in G$ elem inverze az a $g^{-1} \in G$ elem, melyre $g * g^{-1} = g^{-1} * g = e$.

Egy elemnek nem feltétlenül létezik inverze, de ha létezik, akkor egyértelmű. (Miért is? Kell hozzá a művelet asszociativitása!)

## Definíció (Csoport)

Ha a $(G; *)$ egy egységelemes félcsoportban minden $g \in G$ elemnek létezik inverze, akkor $(G; *)$ csoport.

## Definíció (Abel-csoport)

Ha a $(G; *)$ csoportban a $*$ csoportművelet kommutatív, akkor $(G; *)$ Abel-csoport.

$\mathbb{Z}$ a legszűkebb olyan (Abel-) csoport, mely tartalmazza $\mathbb{N}$-et.

# Csoportok

$\mathbb{Z}$ megkonstruálható $\mathbb{N}$-ből: az $(r, s) \sim (p, q)$, ha $r + q = p + s$ ekvivalenciareláció osztályai az egész számok.

Példák csoportokra:

- $(\mathbb{Q}; +)$ a $0$ egységelemmel Abel-csoport.
- $(\mathbb{Q}^*; \cdot)$ az $1$ egységelemmel Abel-csoport, ahol $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.
- $(\mathbb{Z}_m; +)$ a $\overline{0}$ egységelemmel Abel-csoport.
- $(\mathbb{Z}_p^*; \cdot)$ az $\overline{1}$ egységelemmel Abel-csoport.
- $\{M \in \mathbb{C}^{k \times k} : \det M \neq 0\}$ a mátrixszorzással, és az egységmátrixszal mint egységelemmel, csoport (de $k > 1$ esetén nem Abel).
- $X \to X$ bijektív függvények a kompozícióval, és az $id_X : x \mapsto x$ identikus leképzéssel mint egységelemmel.

# Gyűrűk

## Definíció (disztributivitás)

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

## Példa

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

## Szokásos elnevezések, bevett jelölések

$(R; \oplus, \otimes)$ két binér műveletes algebrai struktúra esetén szokás az $\oplus$ műveletet "összeadásnak" és a $\otimes$ műveletet "szorzásnak" nevezni (ha nem okoz félreértést). Az $\oplus$-ra vonatkozó semleges elemet ekkor nullelemnek, a $\otimes$-ra vonatkozó semleges elemet egységelemnek nevezzük. A nullelem szokásos jelölése $0$, az egységelemé $1$, esetleg $e$.

# Gyűrűk

## Definíció (Gyűrű)

Az $(R; \oplus, \otimes)$ két binér műveletes algebrai struktúra gyűrű, ha

- $(R; \oplus)$ Abel-csoport (kommutatív csoport a $0$ egységelemmel);
- $(R; \otimes)$ félcsoport;
- teljesül a $\otimes$-nak a $\oplus$-ra vonatkozó mindkét oldali disztributivitása.

$(R; \oplus, \otimes)$ gyűrű $0$ nulleleme tehát $(R; \oplus)$ Abel-csoport egységeleme.

## Definíció (Egységelemes gyűrű)

Az $(R; \oplus, \otimes)$ gyűrű egységelemes gyűrű, ha $R$-en a $\otimes$ műveletre nézve is van egységelem: $1$ vagy $e$. Azaz ha $(R; \otimes)$ egységelemes félcsoport.

## Definíció (Kommutatív gyűrű)

Az $(R; \oplus, \otimes)$ gyűrű kommutatív gyűrű, ha a $\otimes$ művelet is kommutatív. Azaz ha $(R; \otimes)$ kommutatív félcsoport.

# Gyűrűk

## Példa

- $(\mathbb{Z}; +, \cdot)$ egységelemes kommutatív gyűrű.
- $(2\mathbb{Z}; +, \cdot)$ kommutatív gyűrű, de nem egységelemes.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ a szokásos műveletekkel egységelemes kommutatív gyűrűk.
- $(\mathbb{C}^{k\times k}, +, \cdot)$ a szokásos mátrixösszeadással és mátrixszorzással egységelemes gyűrű, de nem kommutatív, ha $k > 1$.
- $(\mathbb{R}^3; +, \times)$ a 3-dim Euklideszi vektortér a vektoriális szorzással NEM gyűrű mert $\times$ nem asszociatív, ezért $(\mathbb{R}^3; \times)$ nem félcsoport.

## A gyűrűkben általában nem lehet elvégezni az osztást:

- $\mathbb{Z}$-ben nem oldható meg a $2x = 1$ egyenlet.
- $\mathbb{R}^{2\times 2}$-ben nem oldható meg az alábbi egyenlet

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- $\mathbb{Z}_4$-ben nem oldható meg a $2x \equiv 1 \mod 4$.

# Nullosztómentes gyűrűk

## Definíció (Nullosztómentes gyűrű)

Ha egy $(R, \oplus, \otimes)$ gyűrűben $\forall r, s \in R,\ r \neq 0, s \neq 0$ esetén $r \otimes s \neq 0$, akkor $R$ nullosztómentes gyűrű. (Ilyenkor $r \otimes s = 0 \Rightarrow r = 0$ vagy $s = 0$)

## 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. (Mi is az az additív rend?!)

## Definíció (Gyűrű karakterisztikája)

Ha az előző állításban szereplő közös rend $p$, akkor azt mondjuk, hogy a gyűrű karakterisztikája $p$ (jelölése: $\mathrm{char}(R) = p$), ha pedig ez a közös rend végtelen, akkor a gyűrű karakterisztikája $\mathrm{char}(R) = 0$.

# Nullosztómentes gyűrűk

## Definíció

A kommutatív, nullosztómentes gyűrűt integritási tartománynak nevezzük.

## Példa

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

## Definíció

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

## Definíció

Az egységelem osztóját egységnek nevezzük.

Ne keverjük az egységelem és az egység fogalmát! Egységelemből csak egyetlen egy van (az $1$ jelöli), egységből esetleg (tipikusan) több is. (Persze az egységelem mindig egység is, hiszen $1|1$ mivel $1 = 1 \otimes 1$.)

# Testek és Ferdetestek

## Definíció (Ferdetest)

Az $(R; \oplus, \otimes)$ egységelemes gyűrű ferdetest, ha $(R \setminus \{0\}; \otimes)$ csoport.

## Definíció (Test)

A kommutatív ferdetestet (azaz amiben nemcsak az összeadás, hanem a szorzás is kommutatív) testnek nevezzük.

## Példa

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a szokásos műveletekkel testek,
- $\mathbb{Z}_p$ a szokásos műveletekkel test, ha $p$ prím.
- a kvaterniók (Lin.alg.) nem kommutatív ferdetestet alkotnak.

# Gyűrűk

## 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

## 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

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

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

## 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.

## Bizonyítás

$$(f \cdot g)_k = f_0 g_k + f_1 g_{k-1} + \ldots + f_{k-1} g_1 + f_k g_0 =$$
$$= g_k f_0 + g_{k-1} f_1 + \ldots + g_1 f_{k-1} + g_0 f_k =$$
$$= g_0 f_k + g_1 f_{k-1} + \ldots + g_{k-1} f_1 + g_k f_0 = (g \cdot f)_k$$

# Polinomok alapfogalmai

## Állítás

$1 \in R$ egységelem esetén $e = (1, 0, 0 \ldots)$ 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

## Jelölés

Az $f = (f_0, f_1, f_2, \ldots, f_n, 0, 0, \ldots)$, $f_n \neq 0$ $(f_m = 0 : \forall m > n)$ polinomot $f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n$, $f_n \neq 0$ 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 $f = (1, 0, 2, 0, 0, 3, 0, \ldots)$ polinom felírható $f(x) = 1 + 0x + 2x^2 + 0x^3 + 0x^4 + 3x^5$ alakban.
Ugyanezen $f$ további alakjai:
$f(x) = 1 + 2x^2 + 3x^5$, $f(x) = 3x^5 + 2x^2 + 1$.