

Diszkrét matematika 2.C szakirány

5. előadás

Nagy Gábor

nagygabr@gmail.com

nagy@compalg.inf.elte.hu

compalg.inf.elte.hu/~nagy

Komputeralgebra Tanszék

2017. tavasz

Csoportok

Definíció

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

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

Ha ezen felül $*$ kommutatív is, akkor $(G; *)$ **Abel-csoport**.

Példa

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

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

$$\forall k, l, m \in R\text{-re: } k \circ (l * m) = (k \circ l) * (k \circ m), \text{ illetve}$$

$$\forall k, l, m \in R\text{-re: } (l * m) \circ k = (l \circ k) * (m \circ k).$$

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: $\text{char}(R)$.

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

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

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.

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.

Bizonyítás

$$\begin{aligned}(f \cdot g)_k &= f_0 g_k + f_1 g_{k-1} + \dots + f_{k-1} g_1 + f_k g_0 = \\ &= g_k f_0 + g_{k-1} f_1 + \dots + g_1 f_{k-1} + g_0 f_k = \\ &= g_0 f_k + g_1 f_{k-1} + \dots + g_{k-1} f_1 + g_k f_0 = (g \cdot f)_k\end{aligned}$$

Alapfogalmak

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 $g_m \neq 0$.

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

Alapfogalmak

Jelölés

Az $f = (f_0, f_1, f_2, \dots, f_n, 0, 0, \dots)$, $f_n \neq 0$ polinomot
 $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$, $f_n \neq 0$ 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**. A polinom **tagjai** az f_jx^j alakú kifejezések, f_nx^n a **főtagja**, n pedig a **foka**. f fokának jelölésére $\text{deg}(f)$ 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:

$$f(x) = 1 + 2x^2 + 3x^5, f(x) = 3x^5 + 2x^2 + 1.$$

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

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

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 $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n \in R[x]$ polinom $r \in R$ helyen felvett **helyettesítési értékén** az $f(r) = f_0 + f_1r + f_2r^2 + \dots + f_nr^n \in R$ 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 $R \rightarrow R$ 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 $f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0$, ahol $f_n \neq 0$. Ekkor átrendezéssel a következő alakot kapjuk:

$$f(x) = (\dots((f_n \cdot x + f_{n-1}) \cdot x + f_{n-2}) \cdot x + \dots + f_1) \cdot x + f_0, \text{ és így}$$

$$f(c) = (\dots((f_n \cdot c + f_{n-1}) \cdot c + f_{n-2}) \cdot c + \dots + f_1) \cdot c + f_0.$$

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

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

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

Később...

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

Később...

Következmény

Az $f \neq 0$ polinomnak legfeljebb $\deg(f)$ gyöke van.

Bizonyítás

Később...

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

Később...

Következmény

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

Bizonyítás

Később...

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:

$$f = q_1g + r_1;$$

$$g = q_2r_1 + r_2;$$

$$r_1 = q_3r_2 + r_3;$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n;$$

$$r_{n-1} = q_{n+1} r_n.$$

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 $d = u \cdot f + v \cdot g$.