# 6. TÖBBVÁLTOZÓS POLINOMOK

**6.A.Definíció.** Az $\omega = \{0, 1, 2, ..., k, ...\}$ jelölést alkalmazva az $\omega^n = \omega \times \omega \times ... \times \omega$ direkt szorzat (hatvány) halmazból a komplex számok $\mathbb{C}$ halmazába képező

$$f : \omega^n \longrightarrow \mathbb{C}$$

függvényről azt mondjuk, hogy $n$**-változós polinom**, ha $f$ csak véges sok zérustól különböző értéket vesz fel $\mathbb{C}$-ben. A $(k_1, k_2, ..., k_n) \in \omega^n$ egész számokból álló rendezett $n$-es esetén az $f$-nek a $(k_1, k_2, ..., k_n)$ helyen felvett $f_{k_1,k_2,...,k_n} \in \mathbb{C}$ (rendhagyó) módon jelölt függvényértékét nevezzük az $f$ **polinom** $(k_1, k_2, ..., k_n)$ **kitevő sorozathoz tartozó együtthatójának**. A mindenhol 0 értéket felvevő polinomot **zérus polinomnak** nevezzük. Az $n$-változós $f$ és $g$ polinomokra $f = g$ a két függvény egyenlőségét jelenti, vagyis azt, hogy

$$f_{k_1,k_2,...,k_n} = g_{k_1,k_2,...,k_n} \text{ minden } (k_1, k_2, ..., k_n) \in \omega^n \text{ kitevő sorozatra.}$$

Az $\omega^n$ elemein értelmezzünk a $\prec$ relációt az alábbi módon.

$$(k_1, k_2, ..., k_n) \prec (l_1, l_2, ..., l_n),$$

ha létezik egy $1 \leq i \leq n$ index az

$$k_1 = l_1, k_2 = l_2, ..., k_{i-1} = l_{i-1} \text{ és } k_i < l_i$$

tulajdonsággal. Könnyen látható, hogy $\prec$ lineáris rendezése $\omega^n$ elemeinek: szigorúan antiszimmetrikus (azaz $(k_1, k_2, ..., k_n) \prec (l_1, l_2, ..., l_n)$ és $(l_1, l_2, ..., l_n) \prec (k_1, k_2, ..., k_n)$ egyszerre nem teljesül), tranzitív és bármely két különböző elem összehasonlítható. A $\prec$-t nevezzük a **kitevő sorozatok lexikografikus rendezésének**.
Amennyiben $f \neq 0$, akkor a véges sok $f_{k_1,k_2,...,k_n} \neq 0$ tulajdonságú $(k_1, k_2, ..., k_n)$ kitevő sorozat között létezik pontosan egy olyan $(u_1, u_2, ..., u_n)$, amely a $\prec$ lexikografikus rendezésre nézve a legnagyobb, ezt az $f$ **lexikografikusan első kitevő sorozatának** nevezünk. Tehát $f_{u_1,u_2,...,u_n} \neq 0$ és $f_{k_1,k_2,...,k_n} = 0$ minden az $(u_1, u_2, ..., u_n) \prec (k_1, k_2, ..., k_n)$ tulajdonsággal rendelkező $(k_1, k_2, ..., k_n) \in \omega^n$ elemre. A lexikografikusan első kitevő sorozathoz tartozó $f_{u_1,u_2,...,u_n} \neq 0$ együtthatót nevezzük az $f$ polinom **lexikografikus főegyütthatójának**.
Legyen $H \subseteq \mathbb{C}$ tetszőleges részhalmaz, ekkor az $f$ **polinomról** azt mondjuk, hogy $H$**-beli együtthatós**, ha $f_{k_1,k_2,...,k_n} \in H$ minden $(k_1, k_2, ..., k_n) \in \omega^n$ kitevő sorozatra. Nyilvánvaló, hogy a $0 \notin H$ esetben egyetlen $H$-beli együtthatós $n$-változós polinom sem létezik. Amennyiben $\{0, 1\} \subseteq H$, akkor a zérus polinomon kívül említést érdemelnek az alábbi $n$-változós $H$-beli együtthatós $x_i$, $1 \leq i \leq n$ polinomok

$$(x_i)_{k_1,k_2,...,k_n} = \begin{cases} 1, \text{ ha } (k_1, k_2, ..., k_n) = (0, ..., 0, 1, 0, ..., 0) \\ 0, \text{ ha } (k_1, k_2, ..., k_n) \neq (0, ..., 0, 1, 0, ..., 0) \end{cases}$$

(itt $(0, ..., 0, 1, 0, ..., 0)$-ben az 1 az $i$-edik helyen szerepel), ebben az esetben a $H$-beli együtthatós $n$-változós polinomok halmazára a

$$H[x_1, x_2, ..., x_n] = \{f \mid f : \omega^n \longrightarrow H \text{ egy } n\text{-változós polinom}\}$$

jelölést használjuk. Így $\mathbb{C}[x_1, x_2, ..., x_n]$ az összes $n$-változós polinom által alkotott halmazt jelenti.
Az $f$ **polinom** $(\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{C}^n$ **helyen** (komplex számokból álló rendezett $n$-esen) **felvett helyettesítési értékén** az

$$f(\alpha_1, \alpha_2, ..., \alpha_n) = \sum_{(k_1,k_2,...,k_n)\in\omega^n} f_{k_1,k_2,...,k_n} \alpha_1^{k_1} \alpha_2^{k_2} ... \alpha_n^{k_n}$$

komplex számot értjük, ahol az $n$-változós polinom értelmezése miatt az összegezés a véges sok zérustól különböző összeadandóra vonatkozik. Ha $f(\alpha_1, \alpha_2, ..., \alpha_n) = 0$, akkor azt mondjuk, hogy $(\alpha_1, \alpha_2, ..., \alpha_n)$ **zérus helye az $f$-nek**. A helyettesítési érték fenti értelmezése miatt tekintjük az $f$ polinomot az

$$f(x_1, x_2, ..., x_n) = \sum_{(k_1,k_2,...,k_n)\in\omega^n} f_{k_1,k_2,...,k_n} x_1^{k_1} x_2^{k_2} ... x_n^{k_n}$$

algebrai kifejezésként is (amely a polinomok alábbi szorzási szabályát és bizonyos mértékben a $H[x_1, x_2, ..., x_n]$ jelölést is magyarázza). A későbbiekben az $f = f(x_1, x_2, ..., x_n)$ egyenlőségnek a valódi értelme is látható lesz.
Egy polinom szorzása az $a \in \mathbb{C}$ komplex számmal (amely a $(0, 0, ..., 0, ...)$ helyen az $a$ és a többi helyen zérus értéket felvevő $\omega^n \longrightarrow \mathbb{C}$ függvénynek, azaz $n$-változós ún. **konstans polinomnak** is tekinthető) az alábbiak szerint történik:

$$(af)_{k_1,k_2,...,k_n} = a \cdot f_{k_1,k_2,...,k_n}.$$

Az összeadást és kivonást természetes módon értelmezzük polinomokra:

$$(f \pm g)_{k_1,k_2,...,k_n} = f_{k_1,k_2,...,k_n} \pm g_{k_1,k_2,...,k_n}.$$

Az $f(x_1, x_2, ..., x_n)$ és

$$g(x_1, x_2, ..., x_n) = \sum_{(l_1,l_2,...,l_n)\in\omega^n} g_{l_1,l_2,...,l_n} x_1^{l_1} x_2^{l_2} ... x_n^{l_n}$$

szorzatát a többtagú kifejezések szorzásának az elemi algebrából ismert módján értelmezzük:

$$(f_{k_1,k_2,...,k_n} x_1^{k_1} x_2^{k_2} ... x_n^{k_n})(g_{l_1,l_2,...,l_n} x_1^{l_1} x_2^{l_2} ... x_n^{l_n}) = f_{k_1,k_2,...,k_n} g_{l_1,l_2,...,l_n} x_1^{k_1+l_1} x_2^{k_2+l_2} ... x_n^{k_n+l_n} \text{ és}$$

$$(f \cdot g)_{t_1,t_2,...,t_n} = \sum_{k_1+l_1=t_1, k_2+l_2=t_2, ..., k_n+l_n=t_n} f_{k_1,k_2,...,k_n} g_{l_1,l_2,...,l_n},$$

ahol az összegezés a véges számú olyan $(k_1, k_2, ..., k_n), (l_1, l_2, ..., l_n) \in \omega^n$ kitevő sorozatokra vonatkozik, amelyekre $k_1 + l_1 = t_1, k_2 + l_2 = t_2, ..., k_n + l_n = t_n$ teljesül a tekintett $(t_1, t_2, ..., t_n) \in \omega^n$ esetén. Megjegyzésre érdemes, hogy az $a \in \mathbb{C}$ komplex számmal való szorzása $f$-nek ugyanazt az eredményt szolgáltatja, mint az $n$-változós konstans $a$ polinommal való szorzás: $af = a \cdot f$.♡

**6.1.Állítás.** *Az $n$-változós $f$, $g$ és $h$ polinomokra és az $(\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{C}^n$ rendezett $n$-esre az alábbiak teljesülnek.*

1. *$f+g$ és $f-g$ szintén $n$-változós polinomok, továbbá*

$$(f+g)+h=f+(g+h)\ ,\ f+g=g+f\ ,\ (f-g)+g=f\ \text{és}$$

$$(f\pm g)(\alpha_1,\alpha_2,...,\alpha_n)=f(\alpha_1,\alpha_2,...,\alpha_n)\pm g(\alpha_1,\alpha_2,...,\alpha_n).$$

2. *Ha $(k_1,k_2,...,k_n)\prec(k'_1,k'_2,...,k'_n)$ és az $(l_1,l_2,...,l_n)\prec(l'_1,l'_2,...,l'_n)$ vagy a $(l_1,l_2,...,l_n)=(l'_1,l'_2,...,l'_n)$ relációk egyike teljesül, akkor*

$$(k_1+l_1,k_2+l_2,...,k_n+l_n)\prec(k'_1+l'_1,k'_2+l'_2,...,k'_n+l'_n).$$

3. *Ha $f\neq 0\neq g$, akkor $f\cdot g$ olyan $n$-változós polinom, amelynek a lexikografikusan első kitevő sorozata $(u_1+v_1,u_2+v_2,...,u_n+v_n)$, ahol $(u_1,u_2,...,u_n)$ az $f$-nek és $(v_1,v_2,...,v_n)$ a $g$-nek a lexikografikusan első kitevő sorozata. A lexikografikus főegyütthatókra*

$$(f\cdot g)_{u_1+v_1,u_2+v_2,...,u_n+v_n}=f_{u_1,u_2,...,u_n}g_{v_1,v_2,...,v_n}$$

*teljesül. Ez azt is jelenti, hogy az $f\neq 0\neq g$ esetben: $f\cdot g\neq 0$.*

4. $$(f\cdot g)\cdot h=f\cdot(g\cdot h)\ ,\ f\cdot g=g\cdot f\ ,\ (f\pm g)\cdot h=(f\cdot h)\pm(g\cdot h)\ \text{és}$$

$$(f\cdot g)(\alpha_1,\alpha_2,...,\alpha_n)=f(\alpha_1,\alpha_2,...,\alpha_n)g(\alpha_1,\alpha_2,...,\alpha_n).$$

*Az $f_1,f_2,...,f_r\in\mathbb{C}[x_1,x_2,...,x_n]$ polinomokra az $r$-tényezős $f_1\cdot f_2\cdot...\cdot f_r$ szorzat értéke független annak zárójelezésétől.*

*Ha $f\neq 0$ és a $g_1,g_2\in\mathbb{C}[x_1,x_2,...,x_n]$ polinomokra $f\cdot g_1=f\cdot g_2$, akkor $g_1=g_2$.*

5. *Ha $R\subseteq\mathbb{C}$ egy számgyűrű $(\alpha_1,\alpha_2,...,\alpha_n)\in R^n$ és $f,g\in R[x_1,x_2,...,x_n]$, akkor $f\pm g\in R[x_1,x_2,...,x_n]$, $f\cdot g\in R[x_1,x_2,...,x_n]$ és $f(\alpha_1,\alpha_2,...,\alpha_n)\in R$.*

6. *Ha $K\subseteq\mathbb{C}$ egy számtest, $0\neq f\in K[x_1,x_2,...,x_n]$ és $f\cdot g\in K[x_1,x_2,...,x_n]$, akkor $g\in K[x_1,x_2,...,x_n]$.*

**Bizonyítás.** A 2., 3. és a 6.rész igazolására szorítkozunk, a többi rész igazolását az olvasó a definíciók ismeretében könnyen elvégezheti.
A 2.rész igazolása.
$(k_1,k_2,...,k_n)\prec(k'_1,k'_2,...,k'_n)$ azt jelenti, hogy van olyan $1\leq i\leq n$ index, amelyre

$$k_1=k'_1,...,k_{i-1}=k'_{i-1}\ \text{és}\ k_i<k'_i.$$

Ha $(l_1,l_2,...,l_n)=(l'_1,l'_2,...,l'_n)$, akkor

$$k_1+l_1=k'_1+l'_1,...,k_{i-1}+l_{i-1}=k'_{i-1}+l'_{i-1}\ \text{és}\ k_i+l_i<k'_i+l'_i,$$

ami azt jelenti, hogy ilyenkor $(k_1+l_1,k_2+l_2,...,k_n+l_n)\prec(k'_1+l'_1,k'_2+l'_2,...,k'_n+l'_n)$.
Ha $(l_1,l_2,...,l_n)\prec(l'_1,l'_2,...,l'_n)$, akkor van olyan $1\leq j\leq n$ index, amelyre

$$l_1=l'_1,...,l_{j-1}=l'_{j-1}\ \text{és}\ l_j<l'_j.$$

Most a $t = \min\{i, j\}$ indexre

$$k_1 + l_1 = k_1' + l_1', ..., k_{t-1} + l_{t-1} = k_{t-1}' + l_{t-1}' \text{ és } k_t + l_t < k_t' + l_t',$$

ami azt jelenti, hogy $(k_1+l_1, k_2+l_2, ..., k_n+l_n) \prec (k_1'+l_1', k_2'+l_2', ..., k_n'+l_n')$ ebben az esetben is teljesül.
A 3.rész igazolása.
Most

$$(f \cdot g)_{t_1,t_2,...,t_n} = \sum_{k_1+l_1=t_1, k_2+l_2=t_2, ..., k_n+l_n=t_n} f_{k_1,k_2,...,k_n} g_{l_1,l_2,...,l_n}.$$

Ha

$$(u_1 + v_1, u_2 + v_2, ..., u_n + v_n) \prec (k_1 + l_1, k_2 + l_2, ..., k_n + l_n) = (t_1, t_2, ..., t_n),$$

akkor az

$$(u_1, u_2, ..., u_n) \prec (k_1, k_2, ..., k_n) \text{ vagy } (v_1, v_2, ..., v_n) \prec (l_1, l_2, ..., l_n)$$

relációk egyike teljesülni fog, hiszen az ellenkező esetben (mindkét helyen egyenlőség

$$(u_1 + v_1, u_2 + v_2, ..., u_n + v_n) \neq (k_1 + l_1, k_2 + l_2, ..., k_n + l_n)$$

miatt nem állhat) a már igazolt 2.rész szerint a

$$(k_1 + l_1, k_2 + l_2, ..., k_n + l_n) \prec (u_1 + v_1, u_2 + v_2, ..., u_n + v_n)$$

ellentmondáshoz jutnánk. Tehát az $(f \cdot g)_{t_1,t_2,...,t_n}$-et megadó egyenlőség minden összeadandójában $f_{k_1,k_2,...,k_n} = 0$ vagy $g_{l_1,l_2,...,l_n} = 0$, ahonnan $(f \cdot g)_{t_1,t_2,...,t_n} = 0$ adódik.
Ha

$$(u_1 + v_1, u_2 + v_2, ..., u_n + v_n) = (k_1 + l_1, k_2 + l_2, ..., k_n + l_n) = (t_1, t_2, ..., t_n),$$

akkor az alábbi három eset egyike teljesülni fog:

$$(u_1, u_2, ..., u_n) \prec (k_1, k_2, ..., k_n), \text{ vagy}$$

$$(v_1, v_2, ..., v_n) \prec (l_1, l_2, ..., l_n), \text{ vagy}$$

$$(u_1, u_2, ..., u_n) = (k_1, k_2, ..., k_n) \text{ és } (v_1, v_2, ..., v_n) = (l_1, l_2, ..., l_n).$$

Valóban, az ellenkező esetben a már igazolt 2.részt használva a

$$(k_1 + l_1, k_2 + l_2, ..., k_n + l_n) \prec (u_1 + v_1, u_2 + v_2, ..., u_n + v_n)$$

ellentmondáshoz jutnánk. Tehát az $(f \cdot g)_{u_1+v_1,u_2+v_2,...,u_n+v_n}$-et megadó egyenlőség egyetlen összeadandója $f_{u_1,u_2,...,u_n} g_{v_1,v_2,...,v_n}$ különbözik zérustól, ahonnan a kívánt

$$(f \cdot g)_{u_1+v_1,u_2+v_2,...,u_n+v_n} = f_{u_1,u_2,...,u_n} g_{v_1,v_2,...,v_n}$$

egyenlőséget kapjuk.
A 6.rész igazolása.
Tegyük fel, hogy $g \notin K[x_1, x_2, ..., x_n]$ és legyen $(w_1, w_2, ..., w_n)$ a lexikografikusan legnagyobb a $g_{k_1,k_2,...,k_n} \notin K$ tulajdonságú $(k_1, k_2, ..., k_n) \in \omega^n$ kitevő sorozatok között ($0 \in K$ miatt csak

véges sok ilyen létezik). Tekintsük az $f \cdot g$ polinomnak az $(u_1 + w_1, u_2 + w_2, ..., u_n + w_n)$ kitevő sorozathoz tartozó együtthatóját:

$$(f \cdot g)_{u_1+w_1,u_2+w_2,...,u_n+w_n} = \sum_{k_1+l_1=u_1+w_1,k_2+l_2=u_2+w_2,...,k_n+l_n=u_n+w_n} f_{k_1,k_2,...,k_n} g_{l_1,l_2,...,l_n},$$

ahol $(u_1, u_2, ..., u_n)$ továbbra is az $f$-nek a lexikografikusan első kitevő sorozatát jelöli. Megmutatjuk, hogy a fenti összegben $f_{u_1,u_2,...,u_n} g_{w_1,w_2,...,w_n} \notin K$ és ezen kívül minden más összeadandó $K$-beli. Mivel $f \cdot g \in K[x_1, x_2, ..., x_n]$, ezért $(f \cdot g)_{u_1+w_1,u_2+w_2,...,u_n+w_n} \in K$, ami ellentmondás, mert az összeadandók említett tulajdonsága miatt az összeg így nem lehet $K$-beli.
Valóban, $0 \neq f_{u_1,u_2,...,u_n} \in K$, hiszen $(u_1, u_2, ..., u_n)$ az $f \in K[x_1, x_2, ..., x_n]$ polinom lexikografikus főegyütthatója és ezért $g_{w_1,w_2,...,w_n} \notin K$ miatt $f_{u_1,u_2,...,u_n} g_{w_1,w_2,...,w_n} \in K$ nem teljesülhet.
Ha viszont $k_1 + l_1 = u_1 + w_1, k_2 + l_2 = u_2 + w_2, ..., k_n + l_n = u_n + w_n$ teljesül a $(k_1, k_2, ..., k_n) \neq (u_1, u_2, ..., u_n)$ és $(l_1, l_2, ..., l_n) \neq (w_1, w_2, ..., w_n)$ kitevő sorozatokra, akkor vagy

$$(u_1, u_2, ..., u_n) \prec (k_1, k_2, ..., k_n) \text{ és ezzel együtt } f_{k_1,k_2,...,k_n} = 0,$$

vagy

$$(w_1, w_2, ..., w_n) \prec (l_1, l_2, ..., l_n) \text{ és ezzel együtt } g_{l_1,l_2,...,l_n} \in K$$

teljesül $(u_1, u_2, ..., u_n)$ és $(w_1, w_2, ..., w_n)$ választására való tekintettel. Így $f_{k_1,k_2,...,k_n} \in K$ miatt az $f_{k_1,k_2,...,k_n} g_{l_1,l_2,...,l_n} \in K$ tartalmazás mindkét esetben igaz lesz.
Amennyiben a fentiek ellenkezője, azaz

$$(k_1, k_2, ..., k_n) \prec (u_1, u_2, ..., u_n) \text{ és } (l_1, l_2, ..., l_n) \prec (w_1, w_2, ..., w_n)$$

telejesülne, akkor a már igazolt 2.rész alapján az alábbi

$$(k_1 + l_1, k_2 + l_2, ..., k_n + l_n) \prec (u_1 + w_1, u_2 + w_2, ..., u_n + w_n)$$

relációhoz jutnánk, ellentmondásban azzal, hogy

$$(k_1 + l_1, k_2 + l_2, ..., k_n + l_n) = (u_1 + w_1, u_2 + w_2, ..., u_n + w_n).$$

□□□

**6.B.Definíció.** Egy $k \geq 1$ egész számra a $h \in \mathbb{C}[x_1, x_2, ..., x_n]$ **polinom $k$-adik hatványát** a $k$ tényezős

$$h^k = h \cdot h \cdot ... \cdot h$$

szorzat értelmezi (amely a zárójelezésétől független), legyen még $h^0 = 1$. Az $f \in \mathbb{C}[x_1, x_2, ..., x_n]$ **polinom helyettesítési értéke a** $(h_1, h_2, ..., h_n)$ **helyen** (itt $h_1, h_2, ..., h_n \in \mathbb{C}[x_1, x_2, ..., x_n]$) legyen az alábbi

$$f(h_1, h_2, ..., h_n) = \sum_{(k_1,k_2,...,k_n) \in \omega^n} f_{k_1,k_2,...,k_n} h_1^{k_1} h_2^{k_2} ... h_n^{k_n}$$

(itt véges sok zérótól különböző összeadandó van) polinom.♡

**6.2.Állítás.** *Az $f, g, h_1, h_2, ..., h_n \in \mathbb{C}[x_1, x_2, ..., x_n]$ és az $x_i$, $1 \leq i \leq n$ polinomokra az alábbiak teljesülnek.*

1. $(f \pm g)(h_1, h_2, ..., h_n) = f(h_1, h_2, ..., h_n) \pm g(h_1, h_2, ..., h_n)$.
2. $(f \cdot g)(h_1, h_2, ..., h_n) = f(h_1, h_2, ..., h_n) \cdot g(h_1, h_2, ..., h_n)$.
3. *Ha* $(\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{C}^n$, *akkor*
   $(f(h_1,h_2,...,h_n))\,(\alpha_1,\alpha_2,...,\alpha_n) = f\,(h_1(\alpha_1,\alpha_2,...,\alpha_n),h_2(\alpha_1,\alpha_2,...,\alpha_n),...,h_n(\alpha_1,\alpha_2,...,\alpha_n))$.
4. $f(x_1, x_2, ..., x_n) = f$.
5. *Ha* $R \subseteq \mathbb{C}$ *egy számgyűrű és* $f, h_1, h_2, ..., h_n \in R[x_1, x_2, ..., x_n]$, *akkor*
   $f(h_1, h_2, ..., h_n) \in R[x_1, x_2, ..., x_n]$.

**Bizonyítás.** Az olvasó mindegyik rész igazolását a definíciók ismeretében könnyen elvégezheti.

□□□

**Megállapodás.** A most látott 6.2.Állítás 4.része alapján a továbbiakban az $f \in \mathbb{C}[x_1, x_2, ..., x_n]$ $n$-változós polinomot mindenkor az

$$f(x_1, x_2, ..., x_n) = \sum_{(k_1,k_2,...,k_n)\in\omega^n} f_{k_1,k_2,...,k_n} x_1^{k_1} x_2^{k_2} ... x_n^{k_n}$$

alakjában használjuk. A polinomokra megismert műveleti szabályok (lásd a 6.1.Állítást) miatt az ilyen alakban felírt polinomokkal úgy számolhatunk mint az elemi algebrában megszokott többtagú összegekkel.

Az algebrai geometriában alapvető jelentősége van a következő Hilbert-től származó ún. null-hely tételnek, amelyet bizonyítás nélkül közlünk.

**6.3.Tétel (Hilbert Nullstellensatz).** *Az* $f(x_1, x_2, ..., x_n), g_t(x_1, x_2, ..., x_n) \in \mathbb{C}[x_1, x_2, ..., x_n]$, $1 \le t \le m$ *polinomokra az alábbiak ekvivalensek.*

1. $f(\alpha_1, \alpha_2, ..., \alpha_n) = 0$ *minden olyan* $(\alpha_1, \alpha_2, ..., \alpha_n) \in \mathbb{C}^n$ *helyen, ahol* $g_t(\alpha_1, \alpha_2, ..., \alpha_n) = 0$ *teljesül az összes* $1 \le t \le m$ *indexre.*
2. *Léteznek olyan* $u_t(x_1, x_2, ..., x_n) \in \mathbb{C}[x_1, x_2, ..., x_n]$, $1 \le t \le m$ *polinomok és egy olyan* $k \ge 1$ *kitevő, amelyekre*

$$(f(x_1, x_2, ..., x_n))^k = g_1(x_1,x_2,...,x_n)u_1(x_1,x_2,...,x_n) + ... + g_m(x_1,x_2,...,x_n)u_m(x_1,x_2,...,x_n).$$

□□□

**6.C.Definíció.** Az $n$-változós $f(x_1, x_2, ..., x_n) \in \mathbb{C}[x_1, x_2, ..., x_n]$ **polinomot szimmetrikusnak** nevezzük, ha az indexeknek tetszőleges $\pi(1), \pi(2), ..., \pi(n)$ permutációjára polinomoknak az

$$f(x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(n)}) = f(x_1, x_2, ..., x_n)$$

egyenlősége teljesül. Mivel

$$f_{k_1,k_2,...,k_n} x_{\pi(1)}^{k_1} x_{\pi(2)}^{k_2} ... x_{\pi(n)}^{k_n} = f_{k_1,k_2,...,k_n} x_1^{k_{\pi^{-1}(1)}} x_2^{k_{\pi^{-1}(2)}} ... x_n^{k_{\pi^{-1}(n)}},$$

ezért az $f(x_1, x_2, ..., x_n)$ polinom pontosan akkor szimmetrikus, ha tetszőleges $\pi(1), \pi(2), ..., \pi(n)$ permutációra és minden $(k_1, k_2, ..., k_n) \in \omega^n$ kitevő sorozatra teljesül az együtthatók alábbi egyenlősége:

$$f_{k_1,k_2,...,k_n} = f_{k_{\pi^{-1}(1)},k_{\pi^{-1}(2)},...,k_{\pi^{-1}(n)}}.$$

Mivel a $\pi^{-1}$ inverz permutáció is tetszőleges lehet, ezért $\pi^{-1}$ helyett a $\rho$ jelölést alkalmazva kapjuk, hogy az $f(x_1, x_2, ..., x_n)$ polinom pontosan akkor szimmetrikus, ha tetszőleges $\rho(1), \rho(2), ..., \rho(n)$ permutációra és minden $(k_1, k_2, ..., k_n) \in \omega^n$ kitevő sorozatra teljesül az együtthatók alábbi egyenlősége:

$$f_{k_1,k_2,...,k_n} = f_{k_{\rho(1)},k_{\rho(2)},...,k_{\rho(n)}}.$$

Az $a \in \mathbb{C}$ konstans ($n$-változós) polinom nyilvánvalóan szimmetrikus. Az alábbi $n$-változós

$$s_1(x_1, x_2, ..., x_n) = x_1 + x_2 + ... + x_n,$$

$$s_2(x_1, x_2, ..., x_n) = x_1x_2 + x_1x_3 + ... + x_ix_j + ... + x_{n-1}x_n,$$

$$\vdots$$

$$s_t(x_1, x_2, ..., x_n) = x_1x_2...x_t + ... + x_{i_1}x_{i_2}...x_{i_t} + ... + x_{n-t+1}x_{n-t+2}...x_n,$$

$$\vdots$$

$$s_n(x_1, x_2, ..., x_n) = x_1x_2...x_n,$$

polinomokat (amelyeknél $1 \leq i < j \leq n$ és $1 \leq i_1 < i_2 < ... < i_t \leq n$) nevezzük a $\mathbb{C}[x_1, x_2, ..., x_n]$-beli **elemi szimmetrikus polinomoknak**.
Nyilvánvaló, hogy a $t$-edik elemi szimmetrikus polinom olyan $s_t : \omega^n \longrightarrow \mathbb{C}$ függvényt jelent, amelyre $(s_t)_{k_1,k_2,...,k_n} = 1$ minden $t$ darab 1-esből és $n-t$ darab 0-ból álló $(k_1, k_2, ..., k_n) \in \omega^n$ kitevő sorozatra (minden más kitevő sorozaton az $s_t$ értéke 0).♡

**6.4.Állítás.** *Az $F(x_1, x_2, ..., x_n) \in \mathbb{C}[x_1, x_2, ..., x_n]$ polinomra és az $f(x_1, x_2, ..., x_n), g(x_1, x_2, ..., x_n), h_t(x_1, x_2, ..., x_n) \in \mathbb{C}[x_1, x_2, ..., x_n]$, $1 \leq t \leq n$ szimmetrikus polinomokra az alábbiak teljesülnek.*

1. *$f(x_1, x_2, ..., x_n) \pm g(x_1, x_2, ..., x_n), f(x_1, x_2, ..., x_n) \cdot g(x_1, x_2, ..., x_n)$ és $F(h_1, h_2, ..., h_n)$ szintén szimmetrikus polinomok.*

2. *Ha $(u_1, u_2, ..., u_n) \in \omega^n$ az $f(x_1, x_2, ..., x_n)$ polinom lexikografikusan első kitevő sorozata, akkor*

$$u_1 \geq u_2 \geq ... \geq u_n.$$

**Bizonyítás.**

1. Az olvasó ennek a résznek az igazolását a definíciók ismeretében könnyen elvégezheti.

2. Amennyiben valamelyik $1 \leq i \leq n-1$ indexre $u_i < u_{i+1}$ teljesülne, akkor

$$(u_1, ..., u_{i-1}, u_i, u_{i+1}, u_{i+2}, ..., u_n) \prec (u_1, ...u_{i-1}, u_{i+1}, u_i, u_{i+2}..., u_n)$$

és az $f(x_1, x_2, ..., x_n)$ szimmetrikus tulajdonsága miatt

$$f_{u_1,...u_{i-1},u_{i+1},u_i,u_{i+2}...,u_n} = f_{u_1,u_2,...,u_n} \neq 0$$

adódik. Ellentmondásba kerültünk azzal, hogy $(u_1, u_2, ..., u_n) \in \omega^n$ az $f(x_1, x_2, ..., x_n)$ polinom lexikografikusan első kitevő sorozata.

□□□

**6.5.Tétel (a szimmetrikus polinomok alaptétele).** *Ha $R \subseteq \mathbb{C}$ egy számgyűrű, akkor tetszőleges $f(x_1, x_2, ..., x_n) \in R[x_1, x_2, ..., x_n]$ szimmetrikus polinomhoz létezik pontosan egy*

$$f(x_1, x_2, ..., x_n) = F(s_1, s_2, ..., s_n)$$

*tulajdonságú $F(x_1, x_2, ..., x_n) \in R[x_1, x_2, ..., x_n]$ polinom. Tehát minden $R[x_1, x_2, ..., x_n]$-beli szimmetrikus polinom egyértelműen felírható az $s_t(x_1, x_2, ..., x_n)$, $1 \leq t \leq n$ elemi szimmetrikus polinomok $R$-beli együtthatós polinomjaként.*

**Bizonyítás.** Tekintsük az $n$-változós $f(x_1, x_2, ..., x_n)$ szimmetrikus polinomnak a lexikografikusan első $(u_1, u_2, ..., u_n) \in \omega^n$ kitevő sorozatát, ekkor $0 \neq f_{u_1,u_2,...,u_n} \in R$ és az előbbi 6.4.Állítás 2.része szerint $u_1 \geq u_2 \geq ... \geq u_n$.
Az $s_t(x_1, x_2, ..., x_n)$ elemi szimmetrikus polinom lexikografikusan első kitevő sorozata $(1, ..., 1, 0, ..., 0)$, ahol $t$ darab 1-est $n-t$ darab 0 követ. A 6.1.Állítás 3.része alapján egy $r \geq 0$ egész kitevőre az $(s_t(x_1, x_2, ..., x_n))^r$ hatvány lexikografikusan első kitevő sorozata $(\overset{1.}{r}, ..., \overset{t.}{r}, \overset{t+1.}{0}, ..., \overset{n.}{0})$ lesz, ahol $t$ darab $r$-est $n-t$ darab 0 követ.
Ismét a 6.1.Állítás 3.részét használva az

$$f_{u_1,u_2,...,u_n} s_1^{u_1-u_2} s_2^{u_2-u_3} ... s_{n-1}^{u_{n-1}-u_n} s_n^{u_n} \in R[x_1, x_2, ..., x_n]$$

szimmetrikus polinom (itt $s_t(x_1, x_2, ..., x_n)$ kitevőjére $u_t - u_{t+1} \geq 0$ teljesül!) lexikografikusan első kitevő sorozatát az

$$(\overset{1.}{u_t - u_{t+1}}, ..., \overset{t.}{u_t - u_{t+1}}, \overset{t+1.}{0}, ..., \overset{n.}{0}) \text{ és } (u_n, u_n, ..., u_n)$$

kitevő sorozatokból kapjuk:

$$(\overbrace{(u_1 - u_2) + (u_2 - u_3) + ... + (u_{n-1} - u_n) + u_n}^{1.}, ..., \overbrace{(u_t - u_{t+1}) + ... + (u_{n-1} - u_n) + u_n}^{t.}, ..., \overbrace{u_n}^{n.}) =$$

$$= (u_1, ..., u_t, ..., u_n).$$

Tehát $f(x_1, x_2, ..., x_n)$ és $f_{u_1,u_2,...,u_n} s_1^{u_1-u_2} s_2^{u_2-u_3} ... s_{n-1}^{u_{n-1}-u_n} s_n^{u_n}$ lexikografikusan első kitevő sorozata azonos, mindkettő $(u_1, ..., u_t, ..., u_n)$. Így az

$$f_{u_1,u_2,...,u_n} x_1^{u_1-u_2} (x_1 x_2)^{u_2-u_3} ... (x_1 x_2 ... x_{n-1})^{u_{n-1}-u_n} (x_1 x_2 ... x_n)^{u_n} = f_{u_1,u_2,...,u_n} x_1^{u_1} x_2^{u_2} ... x_{n-1}^{u_{n-1}} x_n^{u_n}$$

lexikografikus főtag a

$$g(x_1, x_2, ..., x_n) =$$

$$= f(x_1,x_2, ...,x_n) - f_{u_1,u_2,...,u_n}(s_1(x_1,x_2, ...,x_n))^{u_1-u_2}...(s_{n-1}(x_1,x_2,...,x_n))^{u_{n-1}-u_n}(s_n(x_1,x_2, ...,x_n))^{u_n}$$

különbségből kiesik és olyan $R[x_1, x_2, ..., x_n]$-beli $n$-változós szimmetrikus polinomot kapunk, amelynek a lexikografikusan első $(v_1, v_2, ..., v_n) \in \omega^n$ kitevő sorozatára

$$(v_1, v_2, ..., v_n) \prec (u_1, u_2, ..., u_n).$$

A 6.4.Állítás 2.része szerint $v_1 \geq v_2 \geq ... \geq v_n$ is teljesül. Nyilvánvaló, hogy $v_1 \leq u_1$ miatt a fenti tulajdonságú $(v_1, v_2, ..., v_n)$ kitevő sorozatokból csak véges sok (legfeljebb $(1 + u_1)^n$ darab) van.

Végső soron az $n$-változós $f(x_1, x_2, ..., x_n) \in R[x_1, x_2, ..., x_n]$ szimmetrikus polinomból egy kivonással olyan $n$-változós $g(x_1, x_2, ..., x_n) \in R[x_1, x_2, ..., x_n]$ szimmetrikus polinomot nyertünk, amelynek a lexikografikusan első kitevő sorozata kisebb (a $\prec$ reláció szerint) mint az $f(x_1, x_2, ..., x_n)$-nek a lexikografikusan első kitevő sorozata. Ha az eljárást a $g(x_1, x_2, ..., x_n)$-re újra alkalmazzuk, majd az eredményül kapott $R[x_1, x_2, ..., x_n]$-beli szimmetrikus polinomra ismét elvégezzük az eljárást és aztán tovább folytatjuk az eljárásunk alkalmazását mindig az utoljára kapott eredményre, akkor $R[x_1, x_2, ..., x_n]$-beli szimmetrikus polinomoknak egy olyan sorozatához jutunk, amelyben a lexikografikusan első kitevő sorozatok szigorúan csökkennek a $\prec$ reláció szerint. A fentiek szerint véges sok lépés után a sorozatban olyan $n$-változós polinomhoz jutunk, amelynek a lexikografikusan első kitevő sorozata $(0, 0, ..., 0) \in \omega^n$ (vagy a zérus polinomot kapjuk). Mivel az ilyen polinom konstans, ezért a sorozat előállítása során megtett lépéseket áttekintve megkapjuk az $f(x_1, x_2, ..., x_n)$-nek az előállítását $f_{u_1,u_2,...,u_n} s_1^{u_1-u_2} s_2^{u_2-u_3} ... s_{n-1}^{u_{n-1}-u_n} s_n^{u_n}$ alakú tagok és egy konstans összegeként.

A tételbeli egyértelműség igazolásához elég annyit megmutatni, hogy ha egy $F(x_1, x_2, ..., x_n) \in R[x_1, x_2, ..., x_n]$ polinomra $F(s_1, s_2, ..., s_n) = 0$, akkor $F(x_1, x_2, ..., x_n) = 0$. Ha mégis $F(x_1, x_2, ..., x_n) \neq 0$ teljesülne, akkor tekintsük a

$$(k_1, k_2, ..., k_n) \longmapsto (k_1 + k_2 + ... + k_n, k_2 + ... + k_n, ..., k_{n-1} + k_n, k_n)$$

hozzárendeléssel megadott injektív

$$\{(k_1, k_2, ..., k_n) \in \omega^n \mid F_{k_1,k_2,...,k_n} \neq 0\} \longrightarrow \omega^n$$

függvényt és legyen $(w_1, w_2, ..., w_n)$ az a kitevő sorozat, amelynek ezen függvény szerinti képeleme a lexikografikus rendezésnél a legnagyobb (ilyen a függvényünk értelmezési tartományának végessége miatt létezik). Tehát $F_{w_1,w_2,...,w_n} \neq 0$ és a $(k_1, k_2, ..., k_n) \neq (w_1, w_2, ..., w_n)$ kitevő sorozatra az $F_{k_1,k_2,...,k_n} \neq 0$ esetben

$$(k_1+k_2+...+k_n,k_2+...+k_n,..,k_{n-1}+k_n,k_n) \prec (w_1+w_2+...+w_n,w_2+...+w_n,...,w_{n-1}+w_n,w_n).$$

Az $F(s_1, s_2, ..., s_n)$ polinom lexikografikus főtagját az $F(s_1, s_2, ..., s_n)$ értelmezésében fellépő $F_{w_1,w_2,...,w_n} s_1^{w_1} s_2^{w_2} ... s_n^{w_n}$ összeadandó szolgáltatja:

$$F_{w_1,w_2,...,w_n} x_1^{w_1} (x_1 x_2)^{w_2} ... (x_1 x_2 ... x_n)^{w_n}.$$

A 6.1.Állítás 3.része alapján látjuk, hogy ha $F_{k_1,k_2,...,k_n} \neq 0$, akkor $F_{k_1,k_2,...,k_n} s_1^{k_1} s_2^{k_2} ... s_n^{k_n}$ lexikografikusan első kitevő sorozata

$$(k_1 + k_2 + ... + k_n, k_2 + ... + k_n, ..., k_{n-1} + k_n, k_n),$$

ami $(w_1, w_2, ..., w_n)$ választása miatt a $(k_1, k_2, ..., k_n) = (w_1, w_2, ..., w_n)$ esetben szolgáltatja az $F(s_1, s_2, ..., s_n)$ lexikografikusan első kitevő sorozatát az $F_{w_1,w_2,...,w_n}$ lexikografikus főegyütthatóval. Mivel $F_{w_1,w_2,...,w_n} \neq 0$, ezért az $F(s_1, s_2, ..., s_n) \neq 0$ ellentmondáshoz jutottunk.

□□□

**6.6.Állítás (Viéte képletei).** *Tekintsük a konstanstól különböző $0 \neq a_n \in \mathbb{C}$ főegyütthatóval rendelkező $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{C}[x]$ polinom*

$$f(x) = a_n(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}...(x-\alpha_r)^{k_r}$$

*gyöktényezős felbontását, ahol $\alpha_1, \alpha_2, ..., \alpha_r \in \mathbb{C}$ az $f(x)$ polinom összes gyökeinek egy ismétlődés nélküli felsorolása. Ha $\beta_1, \beta_2, ..., \beta_n \in \mathbb{C}$ ugyanezeknek a gyököknek a multiplicitással történő felsorolása (azaz $\alpha_i$ pontosan $k_i$-szer fordul elő), akkor $n = \deg(f(x))$ és tetszőleges $1 \leq t \leq n$ indexre*

$$s_t(\beta_1, \beta_2, ..., \beta_n) = (-1)^t \frac{a_{n-t}}{a_n},$$

*ahol $s_t(x_1, x_2, ..., x_n)$ a $t$-edik elemi szimmetrikus polinom.*

**Bizonyítás.** Most

$$f(x) = a_n(x-\beta_1)(x-\beta_2)...(x-\beta_n) = a_n(x+(-\beta_1))(x+(-\beta_2))...(x+(-\beta_n))$$

és azonnal látható, hogy a jobboldalon a szorzás elvégzésekor pontosan akkor kapunk $x^{n-t}$-t (azaz $x$-et $n-t$-szer) tartalmazó részlet szorzatot, amikor a $-\beta_1, -\beta_2, ..., -\beta_n$ sorozatból $t$ darab $-\beta_{i_1}, -\beta_{i_2}, ..., -\beta_{i_t}$ (itt $1 \leq i_1 < i_2 < ... < i_t \leq n$) tényezőt választunk és a további $n-t$ darab tényezőt az $x$-ek közül választjuk. Az $x^{n-t}$ együtthatójának a baloldalon és a jobboldalon meg kell egyeznie, ezért

$$a_{n-t} = a_n \sum_{1 \leq i_1 < i_2 < ... < i_t \leq n} (-\beta_{i_1})(-\beta_{i_2})...(-\beta_{i_t}) = (-1)^t a_n s_t(\beta_1, \beta_2, ..., \beta_n).$$

Teljes indukcióval is bizonyíthatjuk az állításunkat az

$$(x-\beta_1)(x-\beta_2)...(x-\beta_n) = \sum_{t=0}^{n} (-1)^t s_t(\beta_1, \beta_2, ..., \beta_n)x^{n-t}$$

indukciós feltevést (itt $s_0 = 1$) használva és ezt $(x-\beta_{n+1})$-el szorozva kapjuk, hogy

$$(x-\beta_1)(x-\beta_2)...(x-\beta_n)(x-\beta_{n+1}) =$$

$$= \sum_{t=0}^{n} (-1)^t s_t(\beta_1, \beta_2, ..., \beta_n)x^{n-t+1} - \sum_{t=0}^{n} (-1)^t s_t(\beta_1, \beta_2, ..., \beta_n)\beta_{n+1}x^{n-t} =$$

$$= \sum_{t=0}^{n} (-1)^t s_t(\beta_1, \beta_2, ..., \beta_n)x^{(n+1)-t} - \sum_{t=1}^{n+1} (-1)^{t-1} s_{t-1}(\beta_1, \beta_2, ..., \beta_n)\beta_{n+1}x^{n-(t-1)} =$$

$$= \sum_{t=0}^{n+1} (-1)^t \{ s_t(\beta_1, \beta_2, ..., \beta_n) + s_{t-1}(\beta_1, \beta_2, ..., \beta_n) \beta_{n+1} \} \, x^{(n+1)-t} = \sum_{t=0}^{n+1} (-1)^t S_t(\beta_1, \beta_2, ..., \beta_n, \beta_{n+1}) x^{n-t},$$

ahol $s_{-1} = s_{n+1} = 0$ és $S_t(x_1, x_2, ..., x_n, x_{n+1})$ a $t$-edik $n+1$ változós elemi szimmetrikus polinom. A fentiek során felhasználtuk a nyilvánvaló

$$S_t(x_1, x_2, ..., x_n, x_{n+1}) = s_t(x_1, x_2, ..., x_n) + s_{t-1}(x_1, x_2, ..., x_n) x_{n+1}$$

azonosságot.

□□□