3. EGYVÁLTOZÓS POLINOMOK

3.A.Definíció. Komplex számok egy $f = (a_0, a_1, ..., a_k, ...)$ végtelen sorozatáról azt mondjuk, hogy **polinom**, ha létezik olyan $m \geq 0$ egész, hogy minden $k \geq m$ indexre $a_k = 0$. Az $a_k \in \mathbb{C}$ számot nevezzük az f **polinom k-ad fokú együtthatójának**. A 0-tól különböző számot nem tartalmazó $0 = (0, 0, ..., 0, ...)$ polinomot **zérus polinomnak** nevezzük. Az f és $g = (b_0, b_1, ..., b_k, ...)$ polinomokra $f = g$, ha $a_k = b_k$ minden $k \geq 0$ egész számra. Amennyiben $f \neq 0$, akkor a legnagyobb indexű nem zérus $a_n \neq 0$ együtthatót nevezzük az f **polinom főegyütthatójának** és ennek indexét n-et a **polinom fokszámának**, ilyenkor

$$0 = a_{n+1} = a_{n+2} = ... = a_k = ...$$

és a fokszámra a $\deg(f) = n$ jelölést alkalmazzuk: $\deg(f) \geq 0$. A **zérus polinomnak a fokszáma** legyen $-\infty$**.** Ha tudjuk, hogy az f polinom legfeljebb n-ed fokú, akkor ezt a tényt gyakran úgy jelezzük, hogy f-nek csak az első $n + 1$ darab együtthatóját írjuk ki:

$$f = (a_0, a_1, ..., a_n) \Longleftrightarrow \deg(f) \leq n,$$

a zérus polinom esetében $0 = (0, 0, ..., 0)$ tetszőleges (véges) számú zérust írhatunk. Egy $k \geq 0$ egész számra az f **polinom k-ad fokú tagján** az alábbi (az $a_k \neq 0$ esetben pontosan k-ad fokú) polinomot értjük:

$$(\overset{0.}{0}, \overset{1.}{0}, ..., \overset{k-1.}{0}, a_k, ...) = (\overset{0.}{0}, \overset{1.}{0}, ..., \overset{k-1.}{0}, a_k).$$

Legyen $H \subseteq \mathbb{C}$ tetszőleges részhalmaz, ekkor az $f = (a_0, a_1, ..., a_k, ...)$ **polinomról** azt mondjuk, hogy H**-beli együtthatós**, ha $a_k \in H$ teljesül minden $k \geq 0$ egészre. Nyilvánvaló, hogy a $0 \notin H$ esetben egyetlen H-beli együtthatós polinom sem létezik. Amennyiben $\{0, 1\} \subseteq H$, akkor a zérus polinomon kívül említést érdemel a H-beli együtthatós

$$x = (0, 1, 0, 0, ..., 0, ...) = (0, 1)$$

elsőfokú polinom, ebben az esetben a H-beli együtthatós polinomok halmazára a

$$H[x] = \{f \mid f = (a_0, a_1, ..., a_k, ...) \text{ polinom és } a_k \in H \text{ minden } k \geq 0 \text{ egészre}\}$$

jelölést használjuk. Így $\mathbb{C}[x]$ az összes polinom által alkotott halmazt jelenti.
Az $f = (a_0, a_1, ..., a_n)$ **polinom** $\alpha \in \mathbb{C}$ **helyen** (komplex számon) **felvett helyettesítési értékén** az

$$f(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n$$

komplex számot értjük, ahol $n = \deg(f)$. Ha $f(\alpha) = 0$, akkor azt mondjuk, hogy az α **gyöke az** $f(x)$ **polinomnak**. A helyettesítési érték fenti értelmezése miatt tekintjük az $f = (a_0, a_1, ..., a_n)$ polinomot az

$$f(x) = a_0 + a_1x + ... + a_nx^n$$

algebrai kifejezésként is (amely a polinomok alábbi szorzási szabályát és bizonyos mértékben a $H[x]$ jelölést is magyarázza). A későbbiekben az $f = f(x)$ egyenlőségnek a valódi értelmét is látni fogjuk.

Az összeadást, kivonást és a szorzást az alábbi módon értelmezzük polinomokra:

$$f \pm g = (a_0 \pm b_0, a_1 \pm b_1, ..., a_k \pm b_k, ...) \text{ és } f \cdot g = (u_0, u_1, ..., u_k, ...),$$

ahol a $k \geq 0$ indexre

$$u_k = a_0b_k + a_1b_{k-1} + ... + a_{k-1}b_1 + a_kb_0 = \sum_{i=0}^{k} a_ib_{k-i}$$

Nyilvánvaló, hogy $f \pm 0 = 0 \pm f = f$, $f - f = 0$, $f \cdot 0 = 0 \cdot f = 0$, továbbá az $a, b \in \mathbb{C}$ számokkal $(a) \pm (b) = (a \pm b)$, $(a) \cdot (b) = (ab)$ és $(a) \cdot f = f \cdot (a) = (aa_0, aa_1, ..., aa_k, ...)$, $f \cdot (1) = (1) \cdot f = f$. Az előbbiek szerint az (a) alakú polinomok a műveletekre nézve úgy viselkednek mint az őket megadó komplex számok, ezért nem okoz félreértést, ha az a számot és az (a) polinomot az azonosítjuk:

$$(a) = (a, 0, 0, ..., 0, ...) = a.$$

Ha az f polinom nulladfokú vagy zérus ($\iff \deg(f) \leq 0$), akkor $f = (f(0)) = f(0)$ és ilyenkor azt mondjuk, hogy f **konstans polinom**.♡

3.1.Állítás. *Az $\alpha \in \mathbb{C}$ komplex számra, az $f = (a_0, a_1, ..., a_k, ...)$, $g = (b_0, b_1, ..., b_k, ...)$ és a $h = (c_0, c_1, ..., c_k, ...)$ polinomokra az alábbiak teljesülnek.*

1. *$f + g$ és $f - g$ olyan polinomok, amelyekre*

   $$\deg(f + g) \leq \max\{\deg(f), \deg(g)\} \text{ és } \deg(f - g) \leq \max\{\deg(f), \deg(g)\}.$$

   Amennyiben $\deg(f) \neq \deg(g)$, akkor a fenti egyenlőtlenségekben egyenlőség teljesül.

   Amennyiben $n = \deg(f) = \deg(g)$ és $a_n = b_n$ (azaz, ha az n-ed fokú tagok megegyeznek), akkor $\deg(f - g) \leq n - 1$.

2. *$(f + g) + h = f + (g + h)$, $f + g = g + f$, $(f - g) + g = f$ és $(f \pm g)(\alpha) = f(\alpha) \pm g(\alpha)$.*

3. *$f \cdot g$ olyan polinom, amelyre $\deg(f \cdot g) = \deg(f) + \deg(g)$.*

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

4. *$(f \cdot g) \cdot h = f \cdot (g \cdot h)$, $f \cdot g = g \cdot f$, $(f \pm g) \cdot h = (f \cdot h) \pm (g \cdot h)$ és $(f \cdot g)(\alpha) = f(\alpha)g(\alpha)$.*

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

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

5. *Ha $R \subseteq \mathbb{C}$ egy számgyűrű $\alpha \in R$ és $f, g \in R[x]$, akkor $f \pm g \in R[x]$, $f \cdot g \in R[x]$ és $f(\alpha) \in R$.*

Bizonyítás. Ha $f = 0$ vagy $g = 0$, akkor a fenti állítások mindegyike teljesül, tehát a bizonyítás során végig feltételezhetjük, hogy $f = (a_0, a_1, ..., a_n) \neq 0$ egy n-ed fokú és $g = (b_0, b_1, ..., b_m) \neq 0$ egy m-ed fokú polinom.

1. Ha $k > \max\{n, m\}$, akkor $a_k = b_k = 0$, azaz $a_k \pm b_k = 0$. Tehát $f+g$ és $f-g$ polinomok, továbbá $\deg(f \pm g) \leq \max\{n, m\}$ (az $f \pm g = 0$ esetben $-\infty \leq \max\{n, m\}$).

   Ha $\deg(f) \neq \deg(g)$, akkor az $n > m$ esetben $a_n \pm b_n = a_n \neq 0$ és az $m > n$ esetben $a_m \pm b_m = b_m \neq 0$.

   Ha $n = \deg(f) = \deg(g)$ és $a_n = b_n$, akkor $a_n - b_n = 0$ és így $\deg(f - g) \leq n - 1$ adódik.

2. Könnyen igazolható.

3. Most $a_n b_m \neq 0$ és $k \geq n + m + 1$ esetén az alábbi

$$b_{n+m} = b_{n+m-1} = ... = b_{m+1} = 0,$$

$$0 = a_{n+1} = ... = a_{n+m-1} = a_{n+m} = ... = a_{k-1} = a_k,$$
$$b_k = b_{k-1} = ... = b_{k-n} = ... = b_{m+1} = 0$$

   egyenlőségek miatt

$$u_{n+m}=a_0b_{n+m}+a_1b_{n+m-1}+...+a_{n-1}b_{m+1}+a_nb_m+a_{n+1}b_{m-1}+...+a_{n+m-1}b_1+a_{n+m}b_0=a_nb_m,$$

   valamint

$$u_k = a_0b_k + a_1b_{k-1} + ... + a_nb_{k-n} + a_{n+1}b_{k-n-1} + ... + a_{k-1}b_1 + a_kb_0 = 0.$$

   Tehát $f \cdot g$ polinom, továbbá $\deg(f \cdot g) = n + m = \deg(f) + \deg(g)$.

4. Az $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ azonosság igazolására szorítkozunk, innen a 14.2.Állítás szerint következik az $f_1 \cdot f_2 \cdot ... \cdot f_r$ szorzatnak a zárójelezéstől való függetlensége.

   Az $(f \cdot g) \cdot h$ polinom l-ed fokú együtthatója

$$w_l' = u_0c_l + u_1c_{l-1} + ... + u_kc_{l-k} + ... + u_{l-1}c_1 + u_lc_0 = (a_0b_0)c_k + (a_0b_1 + a_1b_0)c_{k-1} + ...$$

$$... + (a_0b_k + a_1b_{k-1} + ... + a_ib_{k-i} + ... + a_{k-1}b_1 + a_kb_0)c_{l-k} + ...$$
$$... + (a_0b_{l-1} + a_1b_{l-2} + ... + a_{l-2}b_1 + a_{l-1}b_0)c_1 + (a_0b_l + a_1b_{l-1} + ... + a_{l-1}b_1 + a_lb_0)c_0 =$$
$$= \sum_{0 \leq i \leq k \leq l} a_ib_{k-i}c_{l-k}.$$

   Legyen $g \cdot h = (v_0, v_1, ..., v_k, ...)$, ekkor

$$v_k = b_0c_k + b_1c_{k-1} + ... + b_{k-1}c_1 + b_kc_0$$

   és az $f \cdot (g \cdot h)$ polinom l-ed fokú együtthatója

$$w_l'' = a_0v_l + a_1v_{l-1} + ... + a_iv_{l-i} + ... + a_{l-1}v_1 + a_lv_0 =$$

$$= a_0(b_0c_l + b_1c_{l-1} + ... + b_{l-1}c_1 + b_lc_0) + a_1(b_0c_{l-1} + b_1c_{l-2} + ... + b_{l-2}c_1 + b_{l-1}c_0) + ...$$
$$... + a_i(b_0c_{l-i} + b_1c_{l-i-1} + ... + b_jc_{l-i-j} + ... + b_{l-i-1}c_1 + b_{l-i}c_0) + ...$$
$$... + a_{l-1}(b_0c_1 + b_1c_0) + a_l(b_0c_0) =$$

$$= \sum_{0\le i\le l, 0\le j\le l-i} a_i b_j c_{l-i-j}.$$

Mindkét összegben az olyan $a_i b_s c_t$ szorzatok szerepelnek, amelyeknél $i \ge 0$, $s \ge 0$, $t \ge 0$ és $i+s+t = l$. Tehát $w'_l = w''_l$ minden $l \ge 0$ egészre, ahonnan $(f \cdot g) \cdot h = f \cdot (g \cdot h)$ következik.

5. Könnyen igazolható.

□□□

3.B.Definíció. Egy $k \ge 1$ egész számra a $h \in \mathbb{C}[x]$ **polinom k-adik hatványát** a k tényezős

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

szorzat értelmezi (amely a zárójelezésétől független). Az $f = (a_0, a_1, ..., a_n)$ **polinom helyettesítési értéke a h helyen** legyen az

$$f(h) = a_0 + a_1 h + ... + a_n h^n$$

polinom.♡

3.2.Állítás. *Az $f, g, h \in \mathbb{C}[x]$ és az $x = (0,1,0,0,...,0,...) = (0,1)$ polinomokra:*

1. $\deg(f(h)) = \deg(f)\deg(h)$ *(itt $f \ne 0 \ne h$).*
2. $(f \pm g)(h) = f(h) \pm g(h)$.
3. $(f \cdot g)(h) = f(h) \cdot g(h)$.
4. *Ha $\alpha \in \mathbb{C}$, akkor $(f(g))(\alpha) = f(g(\alpha))$.*
5. $(f(g))(h) = f(g(h))$.
6. $f(x) = f$.
7. *Ha $R \subseteq \mathbb{C}$ egy számgyűrű és $f, h \in R[x]$, akkor $f(h) \in R[x]$.*

Bizonyítás.

1. Mivel a $0 \le k \le n-1$ egészekre $\deg(a_k) \le 0$, ezért a 3.1.Állítás 3.részét használva kapjuk, hogy

   $$\deg(a_k h^k) = \deg(a_k) + k\deg(h) \le k\deg(h) < n\deg(h) = \deg(a_n) + n\deg(h) = \deg(a_n h^n),$$

   ahonnan a 3.1.Állítás 1.részére való tekintettel

   $$\deg(f(h)) = \deg(a_0 + a_1 h + ... + a_n h^n) = \deg(a_n h^n) = n\deg(h) = \deg(f)\deg(h)$$

   következik.

2. Könnyen igazolható.

3. Legyen $g=(b_0,b_1,...,b_m)$ és $f\cdot g=(u_0,u_1,...,u_{n+m})$, ekkor a $0\le k\le n+m$ egészekre $u_k=a_0b_k+a_1b_{k-1}+...+a_{k-1}b_1+a_kb_0$. A nyilvánvaló $(a_ih^i)(b_jh^j)=(a_ib_j)h^{i+j}$ egyenlőség és a polinomok szorzásának az összeadásra vonatkozó disztributívitása miatt (lásd a 3.1.Állítás 4.részét) kapjuk, hogy

$$f(h)\cdot g(h)=(a_0+a_1h+...+a_nh^n)(b_0+b_1h+...+b_mh^m)=\sum_{0\le i\le n\ 0\le j\le m}(a_ih^i)(b_jh^j)=$$

$$=\sum_{0\le i\le n\ 0\le j\le m}(a_ib_j)h^{i+j}=\sum_{k=0}^{n+m}\left(\sum_{0\le i\le k}a_ib_{k-i}\right)h^k=u_0+u_1h+...+u_{n+m}h^{n+m}=(f\cdot g)(h).$$

4. A 3.1.Állítás 2.részében és 4.részében található szabályokat alkalmazva kapjuk, hogy

$$(f(g))(\alpha)=(a_0+a_1g+...+a_ng^n)(\alpha)=a_0(\alpha)+(a_1g)(\alpha)+...+(a_ng^n)(\alpha)=$$

$$=a_0(\alpha)+a_1(\alpha)g(\alpha)+...+a_n(\alpha)g^n(\alpha)=a_0+a_1g(\alpha)+...+a_n(g(\alpha))^n=f(g(\alpha)).$$

5. Most a már igazolt (3.2.Állításbeli) 2.rész és 3.rész alapján kapjuk, hogy

$$(f(g))(h)=(a_0+a_1g+...+a_ng^n)(h)=a_0(h)+(a_1g)(h)+...+(a_ng^n)(h)=$$

$$=a_0(h)+a_1(h)g(h)+...+a_n(h)g^n(h)=a_0+a_1g(h)+...+a_n(g(h))^n=f(g(h)).$$

6. A könnyen ellenőrízhető $x^k=(\overset{0.}{0},\overset{1.}{0},...,\overset{k-1.}{0},1)$ egyenlőséget felhasználva kapjuk, hogy

$$f(x)=a_0+a_1x+...+a_nx^n=a_0+a_1(0,1)+...+a_n(\overset{0.}{0},\overset{1.}{0},...,\overset{n-1.}{0},1)=$$

$$=(a_0,0,...,0,...)+(0,a_1,0,...,0,...)+...+(\overset{0.}{0},\overset{1.}{0},...,\overset{n-1.}{0},a_n,0,...,0,...)=$$
$$=(a_0,a_1,...,a_n,0,...,0,...)=(a_0,a_1,...,a_n)=f.$$

7. Könnyen igazolható.

□□□

Megállapodás. A most igazolt 3.2.Állítás 6.része alapján a továbbiakban az

$$f=(a_0,a_1,...,a_n,0,...,0,...)=(a_0,a_1,...,a_n)$$

polinomot mindenkor az $f(x)=a_0+a_1x+...+a_nx^n$ alakjában használjuk, amelynek k-ad fokú tagja az a_kx^k polinom. A polinomokra megismert műveleti szabályok (lásd a 3.1.Állítást) miatt az ilyen alakban felírt polinomokkal úgy számolhatunk mint az elemi algebrában megszokott többtagú összegekkel.

3.3.Tétel (a maradékos osztásról). *Az* $f(x) = a_0 + a_1x + ... + a_nx^n$ *és a nem zérus* $g(x) = b_0 + b_1x + ... + b_mx^m$ *polinomokhoz található egyetlen olyan* $q(x) \in \mathbb{C}[x]$ *és egyetlen olyan* $r(x) \in \mathbb{C}[x]$ *polinom, amelyekre* $\deg(r(x)) \leq \deg(g(x)) - 1$ *és*

$$f(x) = g(x)q(x) + r(x).$$

Tehát a $q_1(x)$ *és az* $r_1(x)$ *polinomokra a* $\deg(r_1(x)) \leq \deg(g(x)) - 1$ *és az* $f(x) = g(x)q_1(x) + r_1(x)$ *feltételek csak a* $q_1(x) = q(x)$ *és* $r_1(x) = r(x)$ *esetben teljesülnek. Amennyiben a* $K \subseteq \mathbb{C}$ *számtestre* $f(x), g(x) \in K[x]$*, akkor* $q(x), r(x) \in K[x]$*.*

Bizonyítás. Nyugodtan feltételezhetjük, hogy $f(x), g(x) \in K[x]$, hiszen a $K = \mathbb{C}$ esetben ez mindenképpen teljesül. Legyen továbbá $m = \deg(g(x))$.
Amennyiben $f(x) = 0$ vagy $n = 0$, akkor az $m = 0$ esetben a $K[x]$-beli

$$q(x) = \frac{a_0}{b_0} \text{ és } r(x) = 0$$

polinomokra $f(x) = g(x)q(x) + r(x)$ és $\deg(r(x)) = -\infty \leq -1 = m - 1 = \deg(g(x)) - 1$.
Amennyiben $f(x) = 0$ vagy $n = 0$, akkor az $m \geq 1$ esetben a $K[x]$-beli

$$q(x) = 0 \text{ és } r(x) = f(x)$$

polinomokra $f(x) = g(x)q(x) + r(x)$ és $\deg(r(x)) \leq 0 \leq m - 1 = \deg(g(x)) - 1$.
Tegyük fel, hogy az $n \geq 0$ egészre minden $\deg(f(x)) \leq n$ tulajdonságú $f(x) \in K[x]$ polinomnak elvégezhető a maradékos osztása a $g(x) \in K[x]$ polinommal, tehát az $f(x) = g(x)q(x) + r(x)$ és $\deg(r(x)) \leq m - 1 = \deg(g(x)) - 1$ feltételek teljesülnek bizonyos $q(x), r(x) \in K[x]$ polinomokra.
Tekintsünk most egy $K[x]$-beli $n + 1$-ed fokú

$$h(x) = c_0 + c_1x + ... + c_nx^n + c_{n+1}x^{n+1}$$

polinomot, ekkor az $n + 1 \leq m - 1$ esetben a $K[x]$-beli

$$q(x) = 0 \text{ és } r(x) = h(x)$$

polinomokra $h(x) = g(x)q(x) + r(x)$ és $\deg(r(x)) = n + 1 \leq m - 1 = \deg(g(x)) - 1$.
Ha $n + 1 \geq m$, akkor a 3.1.Állítás 1.részére való tekintettel a $K[x]$-beli

$$f(x) = h(x) - \frac{c_{n+1}}{b_m}x^{n-m+1}g(x)$$

polinomra $\deg(f(x)) \leq n$, hiszen a $h(x)$-nek és $\frac{c_{n+1}}{b_m}x^{n-m+1}g(x)$-nek azonos a főtagaja:

$$c_{n+1}x^{n+1} = \left(\frac{c_{n+1}}{b_m}x^{n-m+1}\right)(b_mx^m).$$

Az indukciós feltevésünket alkalmazva a fenti $f(x)$-re, olyan $q(x), r(x) \in K[x]$ polinomok létezését kapjuk, amelyekre

$$h(x) - \frac{c_{n+1}}{b_m}x^{n-m+1}g(x) = g(x)q(x) + r(x)$$

és $\deg(r(x)) \leq m-1 = \deg(g(x))-1$. Innen

$$h(x) = (q(x) + \frac{c_{n+1}}{b_m}x^{n-m+1})g(x) + r(x)$$

adódik a $q(x) + \frac{c_{n+1}}{b_m}x^{n-m+1} \in K[x]$ polinommal, ami azt jeleni, hogy $h(x)$-nek is elvégezhető a maradékos osztása $g(x)$-el.
Az egyértelműség igazolásához tételezzük fel, hogy a $q(x)$, $q_1(x)$ és $r(x)$, $r_1(x)$ polinomokra

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x)$$

továbbá, hogy $\deg(r(x)) \leq m-1$ és $\deg(r_1(x)) \leq m-1$. Ekkor

$$r(x) - r_1(x) = g(x)(q_1(x) - q(x)),$$

ami

$$\deg(r(x) - r_1(x)) \leq \max\{\deg(r(x)), \deg(r_1(x))\} \leq m-1,$$
$$\deg(g(x)(q_1(x) - q(x))) = \deg(g(x)) + \deg(q_1(x) - q(x))$$

és $\deg(g(x)) = m$ miatt csakis a $\deg(q_1(x) - q(x)) = -\infty$ esetben teljesülhet. Tehát $q_1(x) - q(x) = 0$, ahonnan $r(x) - r_1(x) = 0$ is következik.

□□□

3.C.Definíció. Legyenek $f(x), g(x) \in \mathbb{C}[x]$ polinomok.

1. Ha $g(x) \neq 0$, akkor a 3.3.Tétel szerint egyértelműen léteznek olyan $q(x) \in \mathbb{C}[x]$ és $r(x) \in \mathbb{C}[x]$ polinomok, amelyekre $f(x) = g(x)q(x)+r(x)$ és $\deg(r(x)) \leq \deg(g(x))-1$. Azt mondjuk, hogy az $f(x)$-nek a $g(x)$-el való maradékos osztásánál $q(x)$ az **osztási hányados** és $r(x)$ az **osztási maradék**.

2. Ha $g(x) \neq 0$ és létezik olyan $q(x) \in \mathbb{C}[x]$ polinom, amelyre $f(x) = g(x)q(x)$, akkor azt mondjuk, hogy $f(x)$ **osztható** $g(x)$-el, vagy azt, hogy $g(x)$ **osztója** $f(x)$-nek. Ilyenkor az $r(x) = 0$ polinomra $f(x) = g(x)q(x) + r(x)$ és $\deg(r(x)) = \deg(0) = -\infty \leq \deg(g(x)) - 1$ teljesül, ami azt jelenti, hogy az $f(x)$-nek a $g(x)$-el való maradékos osztásánál $q(x)$ az osztási hányados és $r(x) = 0$ az osztási maradék. Az oszthatóság jelölése a $g(x) \mid f(x)$ módon történik.

3. Ha $f(x)$ osztható a $g(x) \neq 0$ polinommal és $g(x)$ is osztható az $f(x) \neq 0$ polinommal, azaz $g(x) \mid f(x)$ és $f(x) \mid g(x)$, akkor azt mondjuk, hogy $f(x)$ és $g(x)$ **asszociáltak**, az asszociáltság ekvivalencia reláció, ezért az $f(x) \sim g(x)$ jelölést alkalmazzuk.

4. Az $f(x) \neq 0$ **polinom normált polinomján** az $f^*(x) = \frac{1}{a_n}f(x)$ polinomot értjük, ahol $n = \deg(f(x))$ és az $a_n \neq 0$ szám az $f(x)$ főegyüttthatója. Nyilvánvaló, hogy az $f^*(x)$ főegyüttthatója 1.

5. Azt mondjuk, hogy a $d(x) \neq 0$ polinom **legnagyobb közös osztója** az $f(x)$ és $g(x)$ polinomoknak, ha $d(x) \mid f(x)$ és $d(x) \mid g(x)$, továbbá tetszőleges a $h(x) \mid f(x)$ és $h(x) \mid g(x)$ oszthatóságokat teljesítő $h(x) \neq 0$ polinomra $h(x) \mid d(x)$. Könnyen látható, hogy az $f(x) = 0$ és a $g(x) = 0$ polinomoknak nem létezik legnagyobb közös osztója. Az is nyilvánvaló, hogy a $g(x) \mid f(x)$ esetben az $f(x)$ és $g(x)$ polinomok (egyik) legnagyobb közös osztója $g(x)$.♡

3.4.Állítás (Bezout tétele). *Egy $\alpha \in \mathbb{C}$ komplex számot tekintve a $f(x) = a_0 + a_1x + ... + a_nx^n$ polinomnak az $x - \alpha$ elsőfokú polinommal való maradékos osztásánál az*

$$r(x) = f(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n$$

konstans polinomot kapjuk osztási maradékként. Tehát $f(x) = (x - \alpha)q(x) + f(\alpha)$ egy bizonyos (egyértelműen meghatározott) $q(x) \in \mathbb{C}[x]$ polinomra. Ha az egymástól különböző $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{C}$ komplex számok gyökei az $f(x)$-nek, akkor teljesül az alábbi

$$(x - \alpha_1)(x - \alpha_2)...(x - \alpha_k) \mid f(x)$$

oszthatóság és a $k \leq n$ egyenlőtlenség (egy n-ed fokú polinomnak legfeljebb n különböző gyöke lehet).

Bizonyítás. A 3.3.Tétel szerint az $f(x)$-nek az elsőfokú $x - \alpha$ polinommal való maradékos osztásával olyan (egyértelműen meghatározott) $q(x)$ hányados és $r(x)$ maradék polinomot kapunk, amelyekre

$$f(x) = (x - \alpha)q(x) + r(x)$$

és $\deg(r(x)) \leq \deg(x - \alpha) - 1 = 0$. Tehát $r(x) = c$ konstans polinom. Ha a fenti egyenlőség bal és jobboldalán szereplő polinomoknak tekintjük az α helyen felvett helyettesítési értékét, akkor azt kapjuk, hogy

$$f(\alpha) = (\alpha - \alpha)q(\alpha) + c = c.$$

Ha $f(\alpha_1) = 0$, akkor az előbbiek szerint

$$f(x) = (x - \alpha_1)q_1(x).$$

Mivel α_2 is gyöke $f(x)$-nek, ezért $f(\alpha_2) = (\alpha_2 - \alpha_1)q_1(\alpha_2) = 0$, ahonnan $\alpha_2 - \alpha_1 \neq 0$ miatt $q_1(\alpha_2) = 0$ következik. Így a $q_1(x)$ polinomra és annak α_2 gyökére alkalmazva a fentieket a

$$q_1(x) = (x - \alpha_2)q_2(x)$$

egyenlőséget kapjuk valamilyen $q_2(x)$ polinomra. Az α_3 is gyöke $f(x)$-nek, továbbá

$$f(x) = (x - \alpha_1)q_1(x) = (x - \alpha_1)(x - \alpha_2)q_2(x).$$

Így kapjuk, hogy $f(\alpha_3) = (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)q_2(\alpha_3) = 0$, ahonnan $\alpha_3 - \alpha_1 \neq 0$ és $\alpha_3 - \alpha_2 \neq 0$ miatt $q_2(\alpha_3) = 0$ következik. Az eljárásunkat folytatva az

$$f(x) = (x - \alpha_1)...(x - \alpha_k)q_k(x)$$

egyenlőséghez, illetve a kívánt

$$(x - \alpha_1)(x - \alpha_2)...(x - \alpha_k) \mid f(x)$$

oszthatósághoz jutunk.

□□□

3.5.Állítás. *Az $f(x), f_1(x), f_2(x), g(x), h(x), u(x) \in \mathbb{C}[x]$ polinomokra és a $K \subseteq \mathbb{C}$ számtestre az alábbiak teljesülnek.*

1. *Ha* $g(x) \neq 0$*, akkor legfeljebb egy olyan* $q(x) \in \mathbb{C}[x]$ *polinom van, amelyre* $f(x) = g(x)q(x)$*. Amennyiben* $f(x), g(x) \in K[x]$ *és* $f(x) = g(x)q(x)$*, akkor* $q(x) \in K[x]$ *is teljesül.*

2. *Ha* $g(x)$ *osztója az* $f_1(x), f_2(x)$ *és* $f(x)$ *polinomoknak, akkor* $g(x) \mid f_1(x) \pm f_2(x)$ *és* $g(x) \mid f(x)h(x)$*. Amennyiben* $f(x) \mid u(x)$ *is teljesül, akkor* $g(x) \mid u(x)$*.*

3. *Az* $f(x)$ *és* $g(x)$ *polinomok pontosan akkor asszociáltak, ha létezik olyan* $0 \neq c \in \mathbb{C}$ *szám (konstans polinom), amelyre* $f(x) = cg(x)$ *(ilyenkor* $g(x) = \frac{1}{c}f(x)$*).*

4. *Az* $f(x)$ *és* $g(x)$ *polinomok pontosan akkor asszociáltak, ha* $\deg(f(x)) = \deg(g(x))$ *és* $g(x) \mid f(x)$ *(vagy* $f(x) \mid g(x)$*).*

5. *Az* $f(x) \neq 0 \neq g(x)$ *polinomokra* $(f^*(x))^* = f^*(x)$*,* $(f(x)g(x))^* = f^*(x)g^*(x)$ *és amennyiben* $f(x) \in K[x]$*, akkor* $f^*(x) \in K[x]$ *is teljesül.*

6. *Tetszőleges* $f(x) \neq 0$ *polinomra* $f^*(x) \sim f(x)$ *és amennyiben az* 1 *főegyütthatóval rendelkező* $g(x)$ *polinomra* $g(x) \sim f(x)$*, akkor* $g(x) = f^*(x)$*.*

7. *Ha* $d_1(x), d_2(x) \in \mathbb{C}[x]$ *mindegyike legnagyobb közös osztója az* $f(x)$ *és* $g(x)$ *polinomoknak, akkor* $d_1(x)$ *és* $d_2(x)$ *asszociáltak:* $d_1(x) \sim d_2(x)$*.*

8. *Ha* $d_1(x) \in \mathbb{C}[x]$ *legnagyobb közös osztója az* $f(x)$ *és* $g(x)$ *polinomoknak és a* $d_2(x) \in \mathbb{C}[x]$ *polinomra* $d_1(x) \sim d_2(x)$*, akkor* $d_2(x)$ *is legnagyobb közös osztója az* $f(x)$ *és* $g(x)$ *polinomoknak.*

9. *Ha* $d(x) \in \mathbb{C}[x]$ *legnagyobb közös osztója az* $f(x)$ *és* $g(x)$ *polinomoknak, továbbá az* $\alpha \in \mathbb{C}$ *szám gyöke* $f(x)$*-nek és* $g(x)$*-nek is (*$f(\alpha) = g(\alpha) = 0$*), akkor* α *gyöke a* $d(x)$ *polinomnak is:* $d(\alpha) = 0$*.*

Bizonyítás.

1. Az első állítás a 3.1.Állítás 3.részéből azonnal megkapható. A második állítás a 3.3.Tétel alapján abból következik, hogy most az $f(x) \in K[x]$ polinomnak a $g(x) \in K[x]$ polinommal való maradékos osztásánál $q(x)$ az osztási hányados és $r(x) = 0$ az osztási maradék.

2. Nyilvánvaló.

3. $g(x) \mid f(x)$ és $f(x) \mid g(x)$ miatt $f(x) = g(x)q_1(x)$ és $g(x) = f(x)q_2(x)$ alkalmas $q_1(x)$ és $q_2(x)$ polinomokra. Így

$$\deg(f(x)) = \deg(g(x)) + \deg(q_1(x)) \text{ és } \deg(g(x)) = \deg(f(x)) + \deg(q_2(x)),$$

ahonnan $q_1(x) \neq 0 \neq q_2(x)$ miatt $\deg(f(x)) \geq \deg(g(x))$ és $\deg(g(x)) \geq \deg(f(x))$, illetve $\deg(f(x)) = \deg(g(x))$ adódik. A fentiek alapján $\deg(q_1(x)) = 0$, ami azt jelenti, hogy a $q_1(x) = c \neq 0$ konstans polinomra $f(x) = g(x)q_1(x) = cg(x)$.

Ha viszont $f(x) = cg(x)$, akkor $g(x) = \frac{1}{c}f(x)$ nyilvánvalóan teljesül. Tehát $g(x) \mid f(x)$ és $f(x) \mid g(x)$.

4. Ha $f(x)$ és $g(x)$ asszociáltak, akkor a már igazolt 3.részben láttuk, hogy

   $\deg(f(x)) = \deg(g(x))$.

   Legyen $\deg(f(x)) = \deg(g(x))$ és $g(x) \mid f(x)$, ekkor $f(x) = g(x)q(x)$ és ezáltal $\deg(f(x)) = \deg(g(x)) + \deg(q(x))$ is teljesül valamilyen $q(x) \neq 0$ polinomra. Tehát $\deg(q(x)) = 0$, ami azt jelenti, hogy a $q(x) = c \neq 0$ konstans polinomra $f(x) = g(x)q(x) = cg(x)$. Így a már igazolt 3.részre való tekintettel $f(x) \sim g(x)$.

5. Az $f^*(x)$ polinom főegyütthatója 1, ezért $(f^*(x))^* = \frac{1}{1}f^*(x) = f^*(x)$. Ha az $f(x)$ főegyütthatója $a_n \neq 0$ és $g(x)$ főegyütthatója $b_m \neq 0$, akkor az $f(x)g(x)$ szorzat polinom főegyütthatója a_nb_m és így

$$(f(x)g(x))^* = \frac{1}{a_nb_m}f(x)g(x) = \left(\frac{1}{a_n}f(x)\right)\left(\frac{1}{b_m}g(x)\right) = f^*(x)g^*(x).$$

   Az $f(x) \in K[x]$ esetben $a_n \in K$ is teljesül, ahonnan $f^*(x) = \frac{1}{a_n}f(x) \in K[x]$ adódik.

6. Mivel $f^*(x) = \frac{1}{a_n}f(x)$, ezért az előbbi 3.rész szerint $f^*(x) \sim f(x)$. Ha az 1 főegyütthatóval rendelkező $g(x)$ polinomra $g(x) \sim f(x)$, akkor szintén az előbbi 3.rész szerint

$$g(x) = \frac{1}{c}f(x) = \frac{a_0}{c} + \frac{a_1}{c}x + ... + \frac{a_{n-1}}{c}x^{n-1} + \frac{a_n}{c}x^n$$

   teljesül valamilyen $0 \neq c \in \mathbb{C}$ számra. Most $\frac{a_n}{c} = 1$, ahonnan $c = a_n$ illetve

$$g(x) = \frac{1}{c}f(x) = \frac{1}{a_n}f(x) = f^*(x)$$

   adódik.

7. A legnagyobb közös osztó definíciója alapján nyilvánvaló.

8. $d_2(x) \mid d_1(x)$ és $d_1(x) \mid f(x)$ a jelen állításbeli 2.rész alapján a $d_2(x) \mid f(x)$

   oszthatósághoz vezet. A $d_2(x) \mid d_1(x)$ és $d_1(x) \mid g(x)$ oszthatóságokból hasonlóan kapjuk, hogy $d_2(x) \mid g(x)$. Ha egy $h(x) \neq 0$ polinomra $h(x) \mid f(x)$ és $h(x) \mid g(x)$ teljesül, akkor abból, hogy $d_1(x)$ legnagyobb közös osztó a $h(x) \mid d_1(x)$ oszthatóság adódik. Így $d_1(x) \mid d_2(x)$ és a már használt 2.rész figyelembe vételével kapjuk, hogy $h(x) \mid d_2(x)$.

9. Bezout tétele (3.4.Állítás) szerint $x - \alpha \mid f(x)$ és $x - \alpha \mid g(x)$, ahonnan a legnagyobb közös osztó definíciója alapján $x - \alpha \mid d(x)$ következik. Tehát $d(\alpha) = 0$.

□□□

3.6.Tétel (a legnagyobb közös osztóról). *Legyen $K \subseteq \mathbb{C}$ egy számtest és az $f(x), g(x) \in K[x]$ polinomok egyike különbözzön zérustól: $\{f(x), g(x)\} \neq \{0\}$. Ekkor léteznek olyan $a(x), b(x) \in K[x]$ polinomok, amelyekre a $K[x]$-beli $d(x) = f(x)a(x)+g(x)b(x)$ polinom az $f(x)$ és $g(x)$ polinomoknak egyik legnagyobb közös osztója.*

Bizonyítás. Tekintsük $K[x]$-beli polinomoknak az alábbi halmazát:

$$\mathcal{D} = \{f(x)u(x) + g(x)v(x) \mid u(x), v(x) \in K[x] \text{ és } f(x)u(x) + g(x)v(x) \neq 0\}.$$

Mivel $f(x)$ és $g(x)$ valamelyike zérustól különböző, ezért $\mathcal{D} \neq \varnothing$. A $\mathcal{D}$-beli polinomok fokszámai nem negatív egész számok, ezért kiválaszthatunk egy olyan $\mathcal{D}$-beli

$$d(x) = f(x)a(x) + g(x)b(x) \neq 0$$

polinomot (itt $a(x), b(x) \in K[x]$), amelynek a fokszáma a lehető legkisebb:

$$\deg(d(x)) \leq \deg(f(x)u(x) + g(x)v(x))$$

tetszőleges olyan $u(x), v(x) \in K[x]$ polinomokra, amelyekre $f(x)u(x) + g(x)v(x) \neq 0$.
Ha az $f(x) \in K[x]$ polinomot maradékosan elosztjuk a $d(x) \in K[x]$ polinommal, akkor az

$$f(x) = d(x)q(x) + r(x)$$

egyenlőséget kapjuk a $\deg(r(x)) \leq \deg(d(x)) - 1$ tulajdonsággal rendelkező $q(x), r(x) \in K[x]$ polinomokra. Mivel $1 - a(x)q(x) \in K[x]$ és $-b(x)q(x) \in K[x]$, továbbá

$$r(x) = f(x) - d(x)q(x) = f(x) - (f(x)a(x) + g(x)b(x))q(x) = f(x)(1 - a(x)q(x)) + g(x)(-b(x)q(x)),$$

ezért az $r(x) \neq 0$ esetben $r(x) \in \mathcal{D}$ teljesülne, ami ellentmondana $d(x)$ választásának, vagyis annak, hogy $\deg(d(x)) \leq \deg(r(x))$. Tehát $r(x) = 0$, ami az $f(x) = d(x)q(x)$ következménnyel, azaz a $d(x) \mid f(x)$ oszthatóság teljesülésével jár. Hasonlóan igazolható, hogy $d(x) \mid g(x)$. Amennyiben a $h(x)$ polinomra $h(x) \mid f(x)$ és $h(x) \mid g(x)$, akkor a 3.4.Állítás 2.részére való tekintettel kapjuk a $h(x) \mid f(x)a(x) + g(x)b(x) = d(x)$ oszthatóságot. Végeredményben azt látjuk, hogy $d(x)$ legnagyobb közös osztója az $f(x)$ és $g(x)$ polinomoknak.

□□□

Megállapodás. A most igazolt 3.5.Tétel alapján az $\{f(x), g(x)\} \neq \{0\}$ tulajdonságú $f(x), g(x) \in K[x]$ polinomoknak létezik egy $d(x) = f(x)a(x) + g(x)b(x)$ alakban felírható legnagyobb közös osztója, ahol $a(x), b(x) \in K[x]$. Így a 3.4.Állítás 6.,7. és 8.része alapján az $f(x)$ és $g(x)$ polinomoknak pontosan egy olyan legnagyobb közös osztója létezik, amelynek a főegyütthatója 1. Ez a legnagyobb közös osztó $d^*(x) = \frac{1}{c}d(x)$, ahol $0 \neq c \in K$ a $d(x)$ polinom főegyütthatója. A $d^*(x) = \text{lnko}(f(x), g(x))$ jelölést gyakran fogjuk használni:

$$d^*(x) = \text{lnko}(f(x), g(x)) = \frac{1}{c}d(x) = f(x)\left(\frac{1}{c}a(x)\right) + g(x)\left(\frac{1}{c}b(x)\right) \in K[x].$$

Az $\{f(x), g(x)\} \neq \{0\}$ tulajdonságú $f(x), g(x) \in \mathbb{C}[x]$ **polinomokról** azt mondjuk, hogy **relatív prímek**, ha $\text{lnko}(f(x), g(x)) = 1$.

3.D.Definíció. Az $f(x), g(x) \in \mathbb{C}[x]$ polinomokra teljesüljön $g(x) \neq 0$ és $\deg(f(x)) \geq \deg(g(x))$. Értelmezzük polinomoknak az $(r_k(x))_{k\geq 1}$ sorozatát úgy, hogy $r_1(x) = f(x)$, $r_2(x) = g(x)$ és amennyiben a $k \geq 2$ egészre $r_k(x) \neq 0$, akkor legyen az $r_{k-1}(x)$ polinomnak

az $r_k(x)$ polinommal való osztási hányadosa $q_k(x)$ és osztási maradéka $r_{k+1}(x)$. Tehát $r_{k+1}(x)$ az

$$r_{k-1}(x) = r_k(x)q_k(x) + r_{k+1}(x)$$

egyenlőség és a fokszámokra vonatkozó $\deg(r_{k+1}(x)) \leq \deg(r_k(x)) - 1$ egyenlőtlenség által a 3.3.Tétel miatt egyértelműen meghatározott polinom. Az $r_k(x) = 0$ esetben a sorozat újabb tagját (azaz $r_{k+1}(x)$-et) nem értelmezzük, a rekurzió ilyenkor véget ér. Az $(r_k(x))_{k\geq 1}$ sorozat fenti előállítását nevezzük az $f(x)$ és $g(x)$ polinomokra vonatkozó **Euklidészi algoritmusnak**.♡

3.7.Tétel (az Euklidészi algoritmusról). *Legyen $K \subseteq \mathbb{C}$ egy számtest, ekkor a $\deg(f(x)) \geq \deg(g(x)) \geq 0$ tulajdonságokkal rendelkező $f(x), g(x) \in K[x]$ polinomokra vonatkozó Euklidészi algoritmus olyan $(r_k(x))_{k\geq 1}$ sorozatot szolgáltat, amelyre:*

1. *Létezik olyan $m \geq 2$ egész szám, amelyre*

   $$\deg(r_1(x)) \geq \deg(r_2(x)) > \deg(r_3(x)) > ... > \deg(r_k(x)) > \deg(r_{k+1}(x)) > ... > \deg(r_m(x)) \geq 0$$

   és $r_{m+1}(x) = 0$ (azaz $\deg(r_{m+1}(x)) = -\infty$, továbbá $r_k(x) \neq 0$ minden $1 \leq k \leq m$ indexre) a sorozat utolsóként értelmezett tagja.

2. *Az $r_k(x) \in K[x]$ tartalmazás teljesül a sorozat minden tagjára, azaz minden $1 \leq k \leq m+1$ indexre.*

3. *Minden $1 \leq k \leq m$ egészre léteznek olyan rekurzióval megadható $a_k(x), b_k(x) \in K[x]$ polinomok, amelyekre*

   $$r_k(x) = f(x)a_k(x) + g(x)b_k(x).$$

4. *Az $r_m(x)$ polinom (a sorozat utolsó zérustól különböző tagja) az $f(x)$ és $g(x)$ polinomok legnagyobb közös osztója.*

Bizonyítás.

1. A sorozat értelmezése és a maradékos osztásnak a 3.Tételben leírt tulajdonságai miatt minden lépésben teljesül $\deg(r_{k+1}(x)) \leq \deg(r_k(x)) - 1$, ahonnan a

   $$\deg(r_1(x)) \geq \deg(r_2(x)) > \deg(r_3(x)) > ... > \deg(r_k(x)) > \deg(r_{k+1}(x)) > ...$$

   sorozathoz jutunk. A szigorú csökkenés azt eredményezi, hogy valamilyen $m \geq 2$ indexre $\deg(r_m(x)) \geq 0$ és $\deg(r_{m+1}(x)) < 0$ teljesül. Így $r_m(x) \neq 0$ és $\deg(r_{m+1}(x)) = -\infty$, azaz $r_{m+1}(x) = 0$ adódik.

2. Az alábbiakban bizonyításra kerülő 3.rész nyilvánvaló következménye.

3. $r_1(x) = f(x) = f(x)a_1(x) + g(x)b_1(x)$ és $r_2(x) = g(x) = f(x)a_2(x) + g(x)b_2(x)$, ahol $a_1(x) = b_2(x) = 1 \in K[x]$ és $a_2(x) = b_1(x) = 0 \in K[x]$.

   Ha egy $2 \leq k \leq m$ index esetén már rendelkezésre állnak az

   $$r_{k-1}(x) = f(x)a_{k-1}(x) + g(x)b_{k-1}(x) \text{ és } r_k(x) = f(x)a_k(x) + g(x)b_k(x)$$

egyenlőségeket kielégítő $a_{k-1}(x), b_{k-1}(x), a_k(x), b_k(x) \in K[x]$ polinomok, akkor tekintsük az $r_{k-1}(x) \in K[x]$ polinomnak az $r_k(x) \in K[x]$ polinommal való maradékos osztásánál fellépő $q_k(x) \in K[x]$ osztási hányados (lásd 3.3.Tétel) felhasználásával felírható

$$a_{k+1}(x) = a_{k-1}(x) - a_k(x)q_k(x) \in K[x] \text{ és } b_{k+1}(x) = b_{k-1}(x) - b_k(x)q_k(x) \in K[x]$$

polinomokat. Az $r_{k-1}(x) = r_k(x)q_k(x) + r_{k+1}(x)$ egyenlőség felhasználásával kapjuk, hogy

$$r_{k+1}(x) = r_{k-1}(x) - r_k(x)q_k(x) = (f(x)a_{k-1}(x) + g(x)b_{k-1}(x)) - (f(x)a_k(x) + g(x)b_k(x))q_k(x) =$$

$$= f(x)(a_{k-1}(x) - a_k(x)q_k(x)) + g(x)(b_{k-1}(x) - b_k(x)q_k(x)) = f(x)a_{k+1}(x) + g(x)b_{k+1}(x).$$

4. $r_m(x) \mid r_m(x)$ és $r_{m+1}(x) = 0$ miatt $r_{m-1}(x) = r_m(x)q_m(x) + r_{m+1}(x) = r_m(x)q_m(x)$, ahonnan $r_m(x) \mid r_{m-1}(x)$ következik. Ha egy $2 \leq k \leq m-1$ egészre már tudjuk, hogy $r_m(x) \mid r_{k+1}(x)$ és $r_m(x) \mid r_k(x)$, akkor az $r_{k-1}(x) = r_k(x)q_k(x) + r_{k+1}(x)$ egyenlőségre való tekintettel az $r_m(x) \mid r_{k-1}(x)$ oszthatóság is teljesül. Így lépésenként haladva megkapjuk, hogy $r_m(x) \mid r_2(x) = g(x)$ és $r_m(x) \mid r_1(x) = f(x)$.

   Ha egy $h(x)$ polinomra $h(x) \mid f(x)$ és $h(x) \mid g(x)$, akkor a 3.4.Állítás 2.részére való tekintettel kapjuk a $h(x) \mid f(x)a_m(x) + g(x)b_m(x) = r_m(x)$ oszthatóságot.

□□□

3.8.Tétel. *Az $f(x), g(x), h(x), g_1(x), g_2(x), p(x) \in \mathbb{C}[x]$ zérustól különböző polinomokra teljesülnek az alábbiak.*

1. *Ha $d(x)$ az (egyik) legnagyobb közös osztója az $f(x)$ és $g(x)$ polinomoknak, akkor $d(x)h(x)$ legnagyobb közös osztója az $f(x)h(x)$ és $g(x)h(x)$ polinomoknak:*

$$\text{lnko}(f(x)h(x), g(x)h(x)) = h^*(x) \cdot \text{lnko}(f(x), g(x)).$$

2. *Ha $g_1(x) \mid f(x)$ és $g_2(x) \mid f(x)$, továbbá $g_1(x)$ és $g_2(x)$ relatív prímek (azaz $\text{lnko}(g_1(x), g_2(x)) = 1$), akkor a $g_1(x)g_2(x) \mid f(x)$ oszthatóság is teljesül.*

3. *Ha $p(x) \mid f(x)g(x)$, továbbá $g(x)$ és $p(x)$ relatív prímek (azaz $\text{lnko}(g(x), p(x)) = 1$), akkor a $p(x) \mid f(x)$ oszthatóság is teljesül.*

Bizonyítás.

1. Most $d(x) \sim d^*(x) = \text{lnko}(f(x), g(x))$ és a 3.6.Tétel, illetve az azt követő megállapodás szerint léteznek olyan $a(x), b(x) \in \mathbb{C}[x]$ polinomok, amelyekre

$$d^*(x) = \text{lnko}(f(x), g(x)) = f(x)a(x) + g(x)b(x).$$

   A $d^*(x) \mid f(x)$ és $d^*(x) \mid g(x)$ oszthatóságokból nyilvánvalóan kapjuk a

$$h(x)d^*(x) \mid h(x)f(x) \text{ és } h(x)d^*(x) \mid h(x)g(x)$$

oszthatóságokat. Amennyiben egy $0 \neq u(x) \in \mathbb{C}[x]$ polinomra $u(x) \mid h(x)f(x)$ és $u(x) \mid h(x)g(x)$, akkor a 3.4.Állítás 2.részére való tekintettel kapjuk az

$$u(x) \mid h(x)f(x)a(x) + h(x)g(x)b(x) = h(x)d^*(x)$$

oszthatóságot. Tehát $h(x)d^*(x)$ (az egyik) legnagyobb közös osztója az $f(x)h(x)$ és $g(x)h(x)$ polinomoknak, ahonnan

$$\text{lnko}(f(x)h(x), g(x)h(x)) = (h(x)d^*(x))^* = h^*(x)(d^*(x))^* =$$

$$= h^*(x)d^*(x) = h^*(x) \cdot \text{lnko}(f(x), g(x))$$

adódik. Mivel $d(x) \sim d^*(x)$ miatt $h(x)d(x) \sim h(x)d^*(x)$, ezért $h(x)d(x)$ is legnagyobb közös osztója az $f(x)h(x)$ és $g(x)h(x)$ polinomoknak.

2. A 3.6.Tétel, illetve az azt követő megállapodás szerint léteznek olyan $a(x), b(x) \in \mathbb{C}[x]$ polinomok, amelyekre

$$1 = \text{lnko}(g_1(x), g_2(x)) = g_1(x)a(x) + g_2(x)b(x).$$

A $g_1(x) \mid f(x)$ és $g_2(x) \mid f(x)$ oszthatóságok azt jelentik, hogy az

$$f(x) = g_1(x)q_1(x) \text{ és } f(x) = g_2(x)q_2(x)$$

egyenlőségek teljesülnek valamilyen $q_1(x) \in \mathbb{C}[x]$ és $q_2(x) \in \mathbb{C}[x]$ polinomokra. A legelsőként tekintett egyenlőség $q_1(x)$-el való szorzásával kapjuk a következőket:

$$q_1(x) = g_1(x)q_1(x)a(x) + g_2(x)q_1(x)b(x) = f(x)a(x) + g_2(x)q_1(x)b(x) =$$

$$= g_2(x)q_2(x)a(x) + g_2(x)q_1(x)b(x) = g_2(x)(q_2(x)a(x) + q_1(x)b(x)),$$

ami az

$$f(x) = g_1(x)q_1(x) = g_1(x)g_2(x)(q_2(x)a(x) + q_1(x)b(x))$$

egyenlőséget, illetve a kívánt $g_1(x)g_2(x) \mid f(x)$ oszthatóságot eredményezi.

3. A 3.6.Tétel, illetve az azt követő megállapodás szerint léteznek olyan $a(x), b(x) \in \mathbb{C}[x]$ polinomok, amelyekre

$$1 = \text{lnko}(g(x), p(x)) = g(x)a(x) + p(x)b(x).$$

A $p(x) \mid f(x)g(x)$ oszthatóság azt jelenti, hogy az $f(x)g(x) = p(x)q(x)$ egyenlőség teljesül valamilyen $q(x) \in \mathbb{C}[x]$ polinomra. Az elsőként tekintett egyenlőség $f(x)$-el való szorzásával kapjuk az alábbi

$$f(x) = f(x)g(x)a(x) + f(x)p(x)b(x) =$$

$$= p(x)q(x)a(x) + p(x)f(x)b(x) = p(x)(q(x)a(x) + f(x)b(x))$$

egyenlőséget, ami a kívánt $p(x) \mid f(x)$ oszthatóságot biztosítja.

□□□