7. tétel

A maradékos osztás és euklideszi algoritmus $T[x]$-ben.

A legnagyobb közös osztó és a legkisebb közös többszörös fogalma és tulajdonságai $T[x]$-ben.

Tétel: $\forall$ T test fölötti $f(x)$, $g(x)$ $(g(x) \neq 0)$ polinomhoz egyértelműen léteznek olyan $q(x)$ és $r(x)$ ugyancsak $T[x]$-beli polinomok, amelyekkel

$$f(x) = g(x)\,q(x) + r(x),$$

ahol vagy $r(x) = 0$, vagy $r^\circ < g^\circ$, azaz $0 \leq r^\circ < g^\circ$

BIZ.: ! $f(x)$ és $g(x)$

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

ahol $b_m \neq 0$, azaz $g^\circ = m \geq 0$

Ha $m = 0 \Rightarrow g(x) = b_0 \neq 0 \Rightarrow f(x) = b_0 \frac{1}{b_0} f(x) + 0$ szerint igaz a tétel állítása $\left(q(x) = \frac{1}{b_0} f(x),\ r(x) = 0\right)$.

Feltesszük, h. $m \geq 1$. Ha $f(x) = 0$ v. $f^\circ = n < m \Rightarrow$

$$f(x) = g(x)\,0 + f(x)$$ szerint ismét igaz

a tétel állítása $\left(q(x) = 0,\ r(x) = f(x)\right)$.

Ha $f^\circ = n \geq m$, azaz $n = m + k$ $(k \in \mathbb{N}) \Rightarrow q(x)$ és $r(x)$ létezését k-szerinti indukcióval bizonyítjuk.

Legyen $k = 0$, és definiáljuk az $f_1(x)$ polinomot:

$$f_1(x) = f(x) - \frac{a_m}{b_m} g(x).$$

Így

$$f_1(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_0 - \frac{a_m}{b_m}\left(b_m x^m + b_{m-1} x^{m-1} + \dots + b_0\right)$$

Összevonás után látható, h. vagy $f_1(x) = 0$, v. $0 \le f_1^\circ \le m-1 < m = g^\circ$,

azaz $0 \le f_1^{\circ\circ} = 2^{f_1^\circ} \le 2^{m-1} < 2^m = 2^{g^\circ} = g^{\circ\circ}$.

$\Downarrow$

$q(x) = \frac{a_m}{b_m}$ és $r(x) = f_1(x)$ választással teljesül, h.

$f(x) = g(x)\,q(x) + r(x)$ és $0 \le r^{\circ\circ} < g^{\circ\circ}$.

Tfh. $k-1 \ge 0$-ra, azaz $n \le m+k-1$-re már igazoltuk $q(x)$ és $r(x)$ létezését.

Bebizonyítjuk, h. $n = m+k$ esetén is léteznek a feltételt kielégítő $q(x)$ és $r(x)$ polinomok.

! (1) $f_2(x) = f(x) - \frac{a_{m+k}}{b_m} x^k g(x)$

$\Downarrow$

$$f_2(x) = a_{m+k} x^{m+k} + \dots + a_0 - \frac{a_{m+k}}{b_m} x^k \left(b_m x^m + \dots + b_0\right).$$

Vagy az $f_2(x) = 0$, vagy $0 \le f_2^\circ \le m+k-1$. Indukciós feltevés szerint $f_2(x)$-höz $\exists$ $q'(x)$ és $r'(x)$ $T[x]$-beli polinom, amelyre

(2) $$f_2(x) = g(x)\,q'(x) + r'(x)$$

és $0 \le r'^{\circ\circ} < g^{\circ\circ}$.

(1)-ből és (2)-ből: $f(x) = g(x)\left(\frac{a_{m+k}}{b_m} x^k + q'(x)\right) + r'(x)$.

A $q(x) = \frac{a_{m+k}}{b_m} x^k + q'(x)$ és $r(x) = r'(x)$ jelöléssel

$$f(x) = g(x)\,q(x) + r(x), \text{ ahol}$$

$0 \le r^{\circ\circ} < g^{\circ\circ}$, azaz v. $r(x) = 0$ v. $0 \le r^\circ < g^\circ$

$\Downarrow$

A maradékos osztás elvégezhetőségét bebizonyítottuk.

Az egyértelműséget indirekt módon bizonyítjuk.

Tfh.

$$(3)\quad \begin{aligned} f(x) &= g(x)\, q_1(x) + r_1(x) \qquad 0 \leq r_1^{\circ\circ} < g^{\circ\circ} \\ f(x) &= g(x)\, q_2(x) + r_2(x) \qquad 0 \leq r_2^{\circ\circ} < g^{\circ\circ}, \end{aligned}$$

ahol $q_1(x), q_2(x), r_1(x), r_2(x) \in T[x]$ és $q_1(x) \neq q_2(x)$.

A (3)-asból kivonással kapjuk:

$$(4)\qquad g(x)\big(q_2(x) - q_1(x)\big) = r_1(x) - r_2(x)$$

Mivel $q_2(x) - q_1(x) \neq 0 \Rightarrow$ (4) bal oldalán álló polinom valódi fokszáma legalább g°, a módosított fokszáma legalább 2^{g°.

A (4) jobb oldalán álló polinom zéruspolinom, v. olyan polinom, amelynek valódi fokszáma kisebb, mint g°, v. a módosított fokszáma kisebb, mint 2^{g°.

A fokszámokban megjelenő ellentmondás oka: $q_1(x) \neq q_2(x)$ feltevés. Ugyanakkor $q_1(x) = q_2(x)$ esetén (4)-ből $r_1(x) = r_2(x)$ adódik.

A tétel egyértelműségére vonatkozó állítását bebizonyítottuk.

Példa:

$$\overbrace{3x^4 - 2x^3 + 3x^2 - x + 1}^{f(x)} : \overbrace{x^2 - 2x + 3}^{g(x)} = \underbrace{3x^2 + 4x + 2}_{q(x)}$$

$$\begin{array}{r} 3x^4 - 2x^3 + 3x^2 - x + 1 \\ -\ \underline{3x^2 - 6x^3 + 9x^2} \qquad\qquad \\ 4x^3 - 6x^2 - x + 1 \\ -\ \underline{4x^3 - 8x^2 + 12x} \qquad \\ 2x^2 - 13x + 1 \\ -\ \underline{2x^2 - 4x + 6} \\ \underbrace{-9x - 5}_{r(x)} \end{array}$$

Tétel: ! $r_n(x)$ az $f(x)$ és $g(x)$ $(g(x) \neq 0)$ $T[x]$-beli polinomokon végrehajtott euklideszi algoritmus utolsó zérustól különböző maradéka. Végtelen sok $X_n(x), Y_n(x) \in T[x]$ polinom létezik, amelyekre: $f(x)X_n(x) + g(x)Y_n(x) = r_n(x)$.

Euklideszi algoritmus:

$$f(x) = g(x) \cdot q_0(x) + r_1(x)$$
$$g(x) = r_1(x) \cdot q_1(x) + r_2(x)$$
$$\vdots$$
$$r_{n-2}(x) = r_{n-1}(x) \cdot q_{n-1}(x) + r_n(x) \qquad g^\circ > r_1^\circ > r_2^\circ > \dots > r_n^\circ$$
$$r_{n-1}(x) = r_n(x) \cdot q_n(x) + 0 \qquad r_n(x) \neq 0$$

$\exists\ X_n(x), Y_n(x) \in T[x]$

$$r_n(x) = f(x)\, X_n(x) + g(x)\, Y_n(x)$$

Def.: Legyen $f(x), g(x) \in T[x]$ és $g(x) \neq 0$. Az $f(x)$ és $g(x)$ polinomok legnagyobb közös osztójának nevezzük a $d(x) \in T[x]$ polinomot, ha:

1) $d(x) \mid f(x)$ és $d(x) \mid g(x)$
2) $f(x)$ és $g(x)$ $\forall\, d'(x) \in T[x]$ közös osztójára igaz, hogy $d'(x) \mid d(x)$

Def.: ! $f(x), g(x) \in T[x]$, és $f(x)g(x) \neq 0$. Az $f(x)$ és $g(x)$ polinomok legkisebb közös többszörösének nevezzük az $m(x) \in T[x]$ polinomot, ha:

1) $f(x) \mid m(x)$ és $g(x) \mid m(x)$

2) $f(x)$ és $g(x)$ $\forall$ $m'(x) \in T[x]$ közös többszörösére igaz, hogy $m(x) \mid m'(x)$.

Tétel: (*) Ha az $f(x)$ és a $g(x)$ $T[x]$-beli polinomoknak van legnagyobb közös osztója, illetve legkisebb közös többszöröse, $\Rightarrow$ ezek asszociáltság erejéig egyértelműen meghatározottak.

Tétel: $\forall$ $f(x), g(x) \in T[x]$ $(g(x) \neq 0)$ polinomoknak $\exists$ lnko, és $g(x) \nmid f(x)$ esetén $(f(x), g(x)) \sim r_n(x)$, ahol $r_n(x)$ az $f(x)$ és $g(x)$ polinomokon végrehajtott euklideszi algoritmus utolsó zérustól különböző maradéka, míg $g(x) \mid f(x)$ esetén $(f(x), g(x)) \sim g(x)$.

BIZ.: Az előző tételből adódik (*), hogy

$g(x) \nmid f(x)$ esetén

$r_n(x) \mid r_{n-1}(x)$, $r_n(x) \mid r_{n-2}(x)$, ... ; $r_n(x) \mid g(x)$, $r_n(x) \mid f(x)$

Ha $d'(x) \mid f(x)$ és $d'(x) \mid g(x)$, $\Rightarrow$ (*) alapján

$d'(x) \mid r_1(x)$, $d'(x) \mid r_2(x)$, ..., $d'(x) \mid r_n(x)$, azaz

$(f(x), g(x)) \sim r_n(x)$.

Ha $g(x) \mid f(x)$ $\Rightarrow$ nyilvánvaló, hogy $(f(x), g(x)) \sim g(x)$.

Tétel: $\forall$ $f(x), g(x)$ és $h(x) \in T[x]$ $(g(x) \neq 0)$ polinomokra igazak az alábbiak.

a., $(f(x), g(x)) \sim (g(x), f(x))$

b., $((f(x), g(x)), h(x)) \sim (f(x), (g(x), h(x)))$

c.; $(g(x), g(x)) \sim g(x)$

d.; $(f(x), g(x))h(x) \sim (f(x)h(x), g(x)h(x))$, ha $h(x) \neq 0$

e.; $(f(x), g(x)) \sim g(x) \Leftrightarrow$, ha $g(x) \mid f(x)$

f.; $(f(x), g(x)) \sim (f(x) + t(x)g(x), g(x))$ $\forall\, t(x) \in T[x]$ esetén.

Def.: ! $f(x), g(x) \in T[x]$ és $g(x) \neq 0$. Ha $(f(x), g(x)) \sim 1 \Rightarrow$ az $f(x)$ és a $g(x)$ polinomokat relatív prímpolinomoknak nevezzük.

Tétel: $\forall\, f(x), g(x) \in T[x]$ $(g(x) \neq 0)$ polinomra

$$\left(\frac{f(x)}{(f(x), g(x))}, \frac{g(x)}{(f(x), g(x))}\right) \sim 1$$

Tétel: ! $f(x), g(x)$ és $h(x) \in T[x]$. Ha $f(x) \mid g(x)h(x)$ és $(f(x), g(x)) \sim 1 \Rightarrow$ $f(x) \mid h(x)$.

Tétel: Bármely $f(x), g(x) \in T[x] \setminus \{0\}$ polinomnak van legkisebb közös többszöröse és

$$[f(x), g(x)] \sim \frac{f(x)g(x)}{(f(x), g(x))}.$$

Tétel: $\forall\, f(x), g(x), h(x) \in T[x] \setminus \{0\}$ polinomra igazak az alábbi tulajdonságok:

a.; $[f(x), g(x)] \sim [g(x), f(x)]$

b.; $[[f(x), g(x)], h(x)] \sim [f(x), [g(x), h(x)]]$

c.; $[f(x), f(x)] \sim f(x)$

d.; $[f(x), g(x)]h(x) \sim [f(x)h(x), g(x)h(x)]$

e.; $[f(x), g(x)] \sim g(x) \Leftrightarrow$, ha $f(x) \mid g(x)$