6. tétel

A test fölötti polinom fogalma. A $T[x]$ polinomgyűrű. Az oszthatóság fogalma és tulajdonságai $T[x]$-ben.

Def.: A T test fölötti (egyhatározatlanú) polinom az

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ alakú (formális) összeget értjük,

ahol $a_n; \dots; a_0 \in T$, x pedig határozatlan.

n a polinom fokszáma. Valódi fokszámról beszélünk, ha $a_n \neq 0$, formális, ha $a_n = 0$. A zérustól különböző T-beli elemek fokszáma 0. A 0-nak vagy nem tulajdonítottunk fokszámot, vagy amint az nekünk a későbbiekben alkalmasabb lesz, a 0 fokszámát $\forall$ más fokszámnál kisebbnek tekintjük. Ez utóbbit formálisan úgy is szokás kifejezni, hogy a 0 fokszáma $-\infty$.

Az a_n a kezdőegyüttható. Ha $a_n = 1 \Rightarrow$ főpolinomról beszélünk.

Ha $c \in T$, akkor $f(x)$ polinomban x helyére c-t írva:

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

T-beli elemet kapjuk, amelyet az $f(x)$ polinom $x = c$ helyen vett helyettesítési értékének nevezzük.

A T test fölötti polinomok halmazát $T[x]$ jelöli.

Módosított fokszám:

$$f^{\circ\circ} := \begin{cases} 2^{f^{\circ}}, & \text{ha } \exists f^{\circ} \\ 0, & \text{ha } \nexists f^{\circ} \end{cases}$$

6. tétel

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

$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$ $T[x]$ - beli két polinom.

Feltehető, hogy $n \geq m$, ezért $g(x)$ a

$g(x) = b_n x^n + \ldots + b_{m+1} x^{m+1} + b_m x^m + \ldots + b_0$ alakban is felvehető,

ahol $b_n = \ldots = b_{m+1} = 0$.

Def.: Két polinom $f(x)$ és $g(x)$ $\Leftrightarrow$ egyenlő, ha a $a_n = b_n$,

$a_{n-1} = b_{n-1}$; ... ; $a_0 = b_0$, azaz a megfelelő együtthatók rendre

egyenlőek.

Def.: A $T[x]$ halmazban a következőképpen definiáljuk az

$f(x)$ és a $g(x)$ polinomok összegét és szorzatát.

I., $f(x)+g(x) := (a_n+b_n)x^n + (a_{n-1}+b_{n-1})x^{n-1} + \ldots + (a_1+b_1)x + (a_0+b_0)$

II., $f(x)\cdot g(x) := a_n b_m \cdot x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \ldots + (a_1 b_0 + a_0 b_1) x + a_0 b_0$

(Az összeadásnál célszerű az alacsonyabb fokszámú polinomot 0 együtthatók segítségével a másikkal megegyező (formális) fokszámú polinommá alakítani)

Látható, hogy összeadással és szorzással újra $T[x]$-beli polinomokat kapunk. Ez azt jelenti, hogy $T[x]$ az összeadásra és a szorzás szerint struktúra, amit $(T[x]; +; \cdot)$ jelöl.

$T[x] := \{ f(x) \mid f(x) = a_n \cdot x^n + \ldots + a_0,\ a_i \in T \}$

Tétel: A $(T[x]; +; \cdot)$ struktúra integritástartomány.

(azaz egységelemes, kommutatív, zérusosztómentes gyűrű)

6/2

(A későbbiekben egyszerűbben a T test fölötti (másképpen T-beli együtthatós) T[x] polinomgyűrűről beszélünk.

BIZ.:

Azt, hogy T[x] kommutatív gyűrű, egyszerű számítással igazolhatjuk. T[x] egységeleme a T test egységeleme, ami a szorzás definíciója alapján egyértelmű. Hasonlóan látható be az összeadás definíciója alapján, hogy T[x] zéruseleme a T zéruseleme.

A zérusosztó-mentességet bizonyítjuk:

Legyen $f(x) \neq 0$ és $g(x) \neq 0$, azaz mindkét polinomban legalább egy együttható különbözik a zérustól. Az általánosság megszorítása nélkül feltehető, hogy $a_n \neq 0$ és $b_m \neq 0$. Tfh: $f(x) \cdot g(x) = 0$, azaz a szorzatpolinom mindegyik együtthatója zérus. Így $a_n b_m = 0$, ami ellentmondás, hiszen a_n, b_m testbeli elemek, és a testben egy szorzat pontosan akkor zérus, ha legalább az egyik tényezője zérus. A kapott ellentmondás bizonyítja állításunkat, és ezzel a tételt is bebizonyítottuk.

A szokásos jelöléseket megtartva:

$$\left.\begin{array}{ll} \mathbb{Q}[x] & : \text{racionális együtthatós} \\ \mathbb{R}[x] & : \text{valós} \quad -\text{"}- \\ \mathbb{C}[x] & : \text{komplex} \quad -\text{"}- \end{array}\right\} \text{polinomgyűrűt jelenti.}$$

Mj.: $(\mathbb{Z}[x]\,;+;\cdot)$ is integritástartomány.

$\mathbb{Z}[x] \subset \mathbb{Q}[x] \subset \mathbb{R}[x] \subset \mathbb{C}[x]$

A polinomok között nincs rendezés, csak a fokszámok között.

Tétel: $f(x)$ osztója $g(x)$-nek, ha $\exists\ h(x)$, amelyre $f(x) \cdot h(x) = g(x)$

$$f(x) \mid g^*(x)$$

Tulajdonságai: (az oszthatóság, mint reláció)

- reflexív ✓ $(f(x) \mid f(x) \quad \forall\ f(x) \in T[x])$
- szimmetrikus – $(f(x) \mid g(x) \not\Rightarrow g(x) \mid f(x))$
- antiszimmetrikus – $(f(x) \mid g(x) \wedge g(x) \mid f(x) \Rightarrow f(x) = g(x))$
- tranzitív ✓ $(f(x) \mid g(x) \wedge g(x) \mid h(x) \Rightarrow f(x) \mid h(x))$
- $f(x) \mid g(x) \wedge g(x) \mid f(x) \Rightarrow f(x) = c \cdot g(x),\ c \in T \setminus \{0\}$

(c: konstans tényező, ami nem zérus, de $\forall$ más szám lehet)

Két polinom asszociált, ha nem 0 konstansban térnek el.

$f(x) \sim g(x)$, ha $\exists\ c \in T[x] \setminus \{0\}$, hogy $f(x) = c \cdot g(x)$

0-val való oszthatóság.

Tétel: az oszthatóságra teljesülnek a következők:

- $f(x) \mid g(x) \wedge f(x) \mid h(x) \Rightarrow f(x) \mid g(x) + h(x)$ az oszthatóság additív tul-a.
- $f(x) \mid g(x) \wedge h(x) \mid j(x) \Rightarrow f(x)h(x) \mid g(x)j(x)$ –"– multiplikatív –"–
- $f(x) \mid 0$
- $0 \mid f(x) \Leftrightarrow$, ha $f(x) = 0$
- Legyen $e(x)$ egy rögzített eleme $T[x]$-nek. Az $e(x)$ polinom osztója $\forall\ f(x) \in T[x]$ polinomnak $\Leftrightarrow$, ha $e(x) \mid 1$, azaz ha $e(x)$ nem zérus T-beli elem.

Def.: A $(T[x]; +; \cdot)$ integritástartomány egy egységelemének osztóit egységeknek nevezzük, továbbá az $f(x)$ és $g(x) \in T[x]$ polinomokat asszociáltaknak nevezzük, ha van olyan $e(x)$ egység $T[x]$-ben, amelyre $f(x) = e(x) \cdot g(x)$.

Ezt a tényt az $f(x) \sim g(x)$ szimbólummal jelöljük.

Tétel: $\forall$ $f(x), g(x) \in T[x]$ esetén

- ha $f(x) | g(x)$ és $g(x) | f(x) \Rightarrow f(x) \sim g(x)$
- ha $f(x) | g(x)$; $f(x) \sim f_1(x) \wedge g(x) \sim g_1(x) \Rightarrow f_1(x) | g_1(x)$.