Klasszikus algebra előadás

Waldhauser Tamás

2014. március 3.

A polinom definíciója

2.26. Definíció.

Az R integritástartomány feletti *polinom*nak olyan R-beli elemekből képezett $(a_0, a_1, \ldots)$ végtelen sorozatot nevezünk, amely csak véges sok nullától különböző tagot tartalmaz. Az a_i elemeket a polinom *együttható*inak nevezzük.

Jelölés.

Az R feletti polinomok halmazát $R[x]$ jelöli.

2.27. Definíció.

- Az $f = (a_0, a_1, \ldots)$ polinom *fokszám*án a legnagyobb olyan n nemnegatív egész számot értjük, amelyre $a_n \neq 0$. Ha nincs ilyen n, azaz ha $f = (0, 0, \ldots)$, akkor azt mondjuk, hogy f fokszáma $-\infty$.
- Ha f fokszáma kisebb, mint 1 (azaz 0 vagy $-\infty$), akkor f-et *konstans* polinomnak nevezzük.
- Ha f foka $n \geq 0$, akkor az $a_n \in R$ elemet f *főegyüttható*jának hívjuk.
- Az olyan polinomot, amelynek főegyütthatója 1, *főpolinom*nak nevezzük.

Jelölés.

Az f polinom fokszámát $\deg f$ jelöli.

Műveletek polinomokkal

2.28. Definíció.

Az $f = (a_0, a_1, \ldots)$ és $g = (b_0, b_1, \ldots)$ polinomok *összeg*ét és *szorzat*át az alábbi képletekkel értelmezzük:

$$f + g = (c_0, c_1, \ldots)\,, \text{ ahol } c_n = a_n + b_n;$$

$$f \cdot g = (d_0, d_1, \ldots)\,, \text{ ahol } d_n = \sum_{i=0}^{n} a_i \cdot b_{n-i}.$$

2.29. Állítás.

Tetszőleges $f, g \in R[x]$ polinomokra

$$\deg(f+g) \leq \max(\deg f, \deg g) \quad \textit{és} \quad \deg(fg) = \deg f + \deg g.$$

2.30. Tétel.

A fent definiált összeadással és szorzással $R[x]$ integritástartomány.

2.31. Definíció.

Az $R[x]$ gyűrűt az R feletti egyhatározatlanú polinomok gyűrűjének, röviden R feletti *polinomgyűrű*nek nevezzük.

De mi az az x?

2.32. Állítás.

Minden $a, b \in R$ esetén

$$(a, 0, 0, \ldots) + (b, 0, 0, \ldots) = (a + b, 0, 0, \ldots)\,;$$

$$(a, 0, 0, \ldots) \cdot (b, 0, 0, \ldots) = (ab, 0, 0, \ldots)\,.$$

Jelölés.

Tetszőleges $a \in R$ esetén az $(a, 0, 0, \ldots)$ polinom helyett egyszerűen a-t írunk, és nem is különböztetjük meg az a gyűrűelemtől. (Úgy tekintjük, hogy $R \subseteq R[x]$.) A $(0, 1, 0, \ldots)$ polinomot pedig x jelöli a továbbiakban.

2.33. Tétel.

Minden nemzéró polinom előáll $a_0 + a_1x + \cdots + a_nx^n$ $(a_n \neq 0)$ alakban, és ez az előállítás egyértelmű. Ha $f = (a_0, a_1, \ldots)$ egy n-edfokú polinom, akkor

$$f = (a_0, a_1, \ldots, a_n, 0, 0, \ldots) = a_0 + a_1x + \cdots + a_nx^n.$$

A polinomgyűrű egységei

Jelölés.

A polinomokat ezentúl $a_n x^n + \cdots + a_1 x + a_0$ vagy $\sum_{i=0}^{n} a_i x^i$ alakban írjuk fel. Egy ilyen felírásnál legtöbbször hallgatólagosan feltesszük, hogy $a_n \neq 0$ (azaz a polinom n-edfokú), valamint hogy $a_{n+1} = a_{n+2} = \ldots = 0$.
Az x szimbólum neve: *határozatlan*. A határozatlant bármilyen más betű is jelölheti, ilyenkor az $R[x]$ jelölés is megfelelően módosul. (Például ha a határozatlan y, akkor a polinomgyűrű $R[y]$.)

2.34. Állítás.

Az $R[x]$ polinomgyűrűben az egységek pontosan azok a konstans polinomok, amelyek (mint R-beli elemek) egységek R-ben. Formálisan: $R[x]^* = R^*$.

Polinom és polinomfüggvény

Az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinomhoz természetes módon tartozik egy

$$f\colon T \to T,\ c \mapsto a_n c^n + \cdots + a_1 c + a_0$$

NEM ÖSSZEKEVERNI!

függvény (az f-hez tartozó polinomfüggvény). Ez azonban NEM azonos az f polinommal!
A polinom egy formális kifejezés (avagy együtthatók sorozata), míg a polinomfüggvény egy leképezés a T halmazon.

Példa.

Tekintsük $\mathbb{Z}_2$ felett az $f = x$ és $g = x^{2014}$ polinomokat. Ez nyilván két különböző polinom (még a fokszámuk is különbözik), de ugyanaz a polinomfüggvény tartozik hozzájuk:

$$f\colon \{\bar{0}, \bar{1}\} \to \{\bar{0}, \bar{1}\}, \quad \bar{0} \mapsto \bar{0}, \qquad \bar{1} \mapsto \bar{1};$$

$$g\colon \{\bar{0}, \bar{1}\} \to \{\bar{0}, \bar{1}\}, \quad \bar{0} \mapsto \bar{0}^{2014}, \quad \bar{1} \mapsto \bar{1}^{2014}.$$

3. Test feletti egyhatározatlanú polinomok

Oszthatóság

3.1. Definíció.

Az $f \in T[x]$ polinom *osztója* a $g \in T[x]$ polinomnak (jelölés: $f \mid g$), ha $\exists h \in T[x]: \ g = fh$.

3.3. Tétel.

Tetszőleges $f, g, h \in T[x]$ polinomokra érvényesek az alábbiak:

(1) $f \mid f$;

(2) $(f \mid g \text{ és } g \mid h) \implies f \mid h$;

(3) $(f \mid g \text{ és } g \mid f) \iff \exists c \in T^* : g = cf$;

(4) $1 \mid f$;

(5) $f \mid 0$;

(6) $f \mid 1 \iff f \in T^*$;

(7) $0 \mid f \iff f = 0$;

(8) $(f \mid g \text{ és } f \mid h) \implies f \mid g \pm h$;

(9) $f \mid g \implies f \mid gh$;

(10) $f \mid g \iff fh \mid gh, \text{ ha } h \neq 0$;

(11) $f \mid g \implies \deg f \leq \deg g, \text{ ha } g \neq 0$.

Oszthatóság (tavalyi)

Definíció.

Az a egész szám *osztója* a b egész számnak (jelölés: $a \mid b$), ha $\exists c \in \mathbb{Z}: \; b = ac$.

Tétel.

Tetszőleges a, b, c egész számokra érvényesek az alábbiak:

(1) $a \mid a$;

(2) $(a \mid b \text{ és } b \mid c) \implies a \mid c$;

(3) $(a \mid b \text{ és } b \mid a) \iff b = \pm a$;

(4) $1 \mid a$;

(5) $a \mid 0$;

(6) $a \mid 1 \iff a = \pm 1$;

(7) $0 \mid a \iff a = 0$;

(8) $(a \mid b \text{ és } a \mid c) \implies a \mid b \pm c$;

(9) $a \mid b \implies a \mid bc$;

(10) $a \mid b \iff ac \mid bc$, *ha* $c \neq 0$;

(11) $a \mid b \implies |a| \leq |b|$, *ha* $b \neq 0$.

Asszociáltság

3.2. Definíció.

Az f és g polinomok *asszociáltak* (jelölés: $f \sim g$), ha $f \mid g$ és $g \mid f$.

3.4. Tétel.

Az asszociáltság ekvivalenciareláció $T[x]$-en. A nulla osztályát kivéve minden asszociáltsági osztály tartalmaz pontosan egy főpolinomot.

Megjegyzés.

Asszociált polinomokat nem érdemes (sőt nem is lehet) megkülönböztetni, ha csak az oszthatóságot vizsgáljuk.

Ha az oszthatósági relációt az asszociáltsági osztályok halmazán értelmezzük, akkor már nemcsak reflexív és tranzitív, hanem antiszimmetrikus is lesz, azaz részbenrendezés. A kapott $(T[x] / \sim; |)$ részbenrendezett halmaz legkisebb eleme $1/\sim = T^*$, legnagyobb eleme $0/\sim = \{0\}$.

Test feletti polinomgyűrű esetén minden asszociáltsági osztály (a nulláét kivéve) pontosan egy főpolinomot tartalmaz, tehát asszociáltság erejéig mindig dolgozhatunk főpolinomokkal.

3.5. Tétel (a maradékos osztás tétele).

Ha $f, g \in T[x]$, és $g \neq 0$, akkor léteznek olyan egyértelműen meghatározott q és $r \in T[x]$ polinomok, amelyekre $f = qg + r$ és $\deg r < \deg g$.

3.6. Definíció.

A $d \in T[x]$ polinom *legnagyobb közös osztó*ja az f és $g \in T[x]$ polinomoknak, ha teljesül a következő két feltétel:

1. $d \mid f$ és $d \mid g$;
2. $\forall k \in T[x] : (k \mid f \text{ és } k \mid g) \implies k \mid d$.

Hasonlóan definiálható polinomok *legkisebb közös többszörös*e is.

3.8. Megjegyzés.

Természetesebbnek tűnhet a legnagyobb közös osztót a legmagasabb fokszámú közös osztóként definiálni. Ha d legnagyobb közös osztója f-nek és g-nek a 3.6. Definíció értelmében és $d \neq 0$, akkor h maximális fokszámú f és g közös osztói között. Valóban, ha k egy közös osztó, akkor $k \mid d$ és így $\deg k \leq \deg d$ (lásd a 3.1. Tételbeli (11) tulajdonságot).