Klasszikus algebra előadás

Waldhauser Tamás
2014. március 10.

Maradékos osztás, Inko

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).

Euklideszi algoritmus

3.7. Tétel.

Bármely két $f, g \in T[x]$ polinomnak létezik legnagyobb közös osztója és legkisebb közös többszöröse, és ezek asszociáltság erejéig egyértelműen meghatározottak. A legnagyobb közös osztó kiszámítható az euklideszi algoritmussal, és kifejezhető f és g „lineáris kombinációjaként": $\exists u, v \in T[x]: \; fu + gv = d$.

Példa.

Határozzuk meg az alábbi két polinom legnagyobb közös osztóját:

$$f = x^4 + 2x^3 + 4x^2 + 2x + 3, \qquad g = x^3 + x^2 + x - 3.$$

$$\begin{aligned} x^4 + 2x^3 + 4x^2 + 2x + 3 &= (x+1) \cdot \left(x^3 + x^2 + x - 3\right) + 2x^2 + 4x + 6 \\ x^3 + x^2 + x - 3 &= (x-1) \cdot \left(x^2 + 2x + 3\right) + 0 \end{aligned}$$

Tehát $\text{Inko}(f, g) \sim x^2 + 2x + 3$.
Hab a tortán:

$$\begin{aligned} f &= \left(x^2+1\right)\left(x^2+2x+3\right), \quad \text{gyökei:} \quad \pm i, \; -1 \pm \sqrt{2}i \\ g &= (x-1)\left(x^2+2x+3\right), \quad \text{gyökei:} \quad 1, \; -1 \pm \sqrt{2}i \end{aligned}$$

Relatív prímség

Definíció.
Azt mondjuk, hogy az $f, g \in T[x]$ polinomok *relatív prím*ek, ha $\operatorname{lnko}(f, g) \sim 1$.

Tétel.
Tetszőleges $0 \neq f, g \in T[x]$ *polinomok esetén* $\frac{f}{\operatorname{lnko}(f,g)}$ *és* $\frac{g}{\operatorname{lnko}(f,g)}$ *relatív prím.*

Tétel.
Tetszőleges $f, g, h \in T[x]$ *esetén ha* f *és* g *relatív prím, akkor* $f \mid gh \iff f \mid h$.

Tétel.
Tetszőleges $f, g, h \in T[x]$ *polinomok esetén ha* $\operatorname{lnko}(f, g) \neq 0$, *akkor*

$$f \mid gh \iff \frac{f}{\operatorname{lnko}(f, g)} \mid h.$$

Diofantoszi egyenlet polinomgyűrűben

3.9. Tétel.

Tetszőleges adott nemzéró $f, g, h \in T[x]$ *polinomok esetén az* $fu + gv = h$ *egyenlet akkor és csak akkor oldható meg az ismeretlen* $u, v \in T[x]$ *polinomokra nézve, ha* $\operatorname{lnko}(f, g) \mid h$.

Ha (u_0, v_0) *egy megoldás, akkor bármely* $t \in T[x]$ *esetén az alábbi* (u, v) *pár is megoldás, továbbá minden megoldás előáll ilyen alakban a* t *polinom alkalmas megválasztásával:*

$$u = u_0 + \frac{g}{\operatorname{lnko}(f, g)} \cdot t;$$

$$v = v_0 - \frac{f}{\operatorname{lnko}(f, g)} \cdot t.$$

Diofantoszi egyenlet polinomgyűrűben

Példa.

Oldjuk meg az $fu + gv = \overline{1}$ egyenletet a $\mathbb{Z}_5[x]$ polinomgyűrűben, ahol

$$f = x^2 + \overline{3}x + \overline{1}, \qquad g = x^3 + \overline{2}x^2 + \overline{4}x + \overline{2}.$$

$$\begin{aligned} x^3 + \overline{2}x^2 + \overline{4}x + \overline{2} &= (x + \overline{4}) \cdot (x^2 + \overline{3}x + \overline{1}) + x + \overline{3} \\ x^2 + \overline{3}x + \overline{1} &= x \cdot (x + \overline{3}) + \overline{1} \\ x + \overline{3} &= (x + \overline{3}) \cdot \overline{1} + \overline{0} \end{aligned}$$

Fejezzük ki $\overline{1}$-et f és g segítségével:

$$\overline{1} = f - x \cdot (x + \overline{3}) = f - x \cdot (g - (x + \overline{4}) \cdot f) = (x^2 + \overline{4}x + \overline{1}) \cdot f - x \cdot g$$

Az egyenlet egy megoldása: $u_0 = x^2 + \overline{4}x + \overline{1}, \quad v_0 = -x.$

Kongruenciareláció

3.10. Definíció.

Tetszőleges $f, g, m \in T[x]$ esetén azt mondjuk, hogy *f kongruens g-vel modulo m* (jelölés $f \equiv g \pmod{m}$), ha $m \mid f - g$.

3.11. Állítás.

A mod m *kongruencia ekvivalenciareláció $T[x]$-en, és két polinom akkor és csak akkor kongruens modulo m, ha ugyanazt a maradékot adják m-mel osztva.*

Tétel.

Tetszőleges $f, g, h, f_1, g_1, f_2, g_2, m \in T[x]$ esetén érvényesek az alábbiak:

- $$\left.\begin{aligned} f_1 &\equiv g_1 \pmod{m} \\ f_2 &\equiv g_2 \pmod{m} \end{aligned}\right\} \Longrightarrow \begin{aligned} f_1 \pm f_2 &\equiv g_1 \pm g_2 \pmod{m} \\ f_1 \cdot f_2 &\equiv g_1 \cdot g_2 \pmod{m} \end{aligned}$$

- *Ha $h \neq 0$, akkor* $hf \equiv hg \pmod{m} \iff f \equiv g \left(\mathrm{mod}\ \frac{m}{\mathrm{lnko}(m,h)}\right)$.

- *Ha* $\mathrm{lnko}(m, h) \sim 1$, *akkor* $hf \equiv hg \pmod{m} \iff f \equiv g \pmod{m}$.

Lineáris kongruencia

3.12. Tétel.

Tetszőleges $f, g, h \in T[x]$ *esetén az* $f \cdot u \equiv h \pmod{m}$ *lineáris kongruencia akkor és csak akkor oldható meg, ha* $\operatorname{lnko}(f, m) \mid h$. *Ha ez teljesül, akkor a megoldások egyetlen modulo* $\frac{m}{\operatorname{lnko}(f,m)}$ *maradékosztályt alkotnak.*

Példa.

Oldjuk meg az $f \cdot u \equiv \overline{1} \pmod{m}$ konruenciát a $\mathbb{Z}_5[x]$ polinomgyűrűben, ahol

$$f = x^2 + \overline{3}x + \overline{1}, \qquad m = x^3 + \overline{2}x^2 + \overline{4}x + \overline{2}.$$

$$\begin{aligned} f \cdot u \equiv \overline{1} \pmod{m} \quad &\Longleftrightarrow \quad \exists v \in \mathbb{Z}_5[x]: \ fu = \overline{1} + mv \\ &\Longleftrightarrow \quad \exists v \in \mathbb{Z}_5[x]: \ fu - mv = \overline{1} \end{aligned}$$

Egy megoldás: $u_0 = x^2 + \overline{4}x + \overline{1}$.

Az általános megoldás: $u \equiv x^2 + \overline{4}x + \overline{1} \pmod{m}$.

Maradékosztály-gyűrű

3.13. Definíció.

A mod m kongruenciához tartozó ekvivalenciaosztályokat modulo m *maradékosztály*oknak nevezzük. Az $f \in T[x]$ polinomot tartalmazó modulo m maradékosztályt $\overline{f}$ jelöli, a maradékosztályok halmazát (vagyis a modulo m kongruenciához tartozó faktorhalmazt) pedig $T[x]/(m)$ jelöli.
Tehát $T[x]/(m) = \left\{\overline{f} : f \in T[x]\right\}$.

3.14. Definíció.

A modulo m maradékosztályok halmazán értelmezzük az összeadást, az additív inverz képzését és a szorzást a következőképpen: tetszőleges $f, g \in T[x]$ esetén legyen

$$\overline{f} + \overline{g} = \overline{f+g}, \quad -\overline{g} = \overline{-g}, \quad \overline{f} \cdot \overline{g} = \overline{f \cdot g}.$$

3.15. Állítás.

A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (additív inverze, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik elemet választjuk reprezentánsnak, és ezekkel a műveletekkel $T[x]/(m)$ kommutatív egységelemes gyűrűt alkot (maradékosztály-gyűrű).

A maradékosztály-gyűrű egységei

3.16. Tétel.

Az $\overline{f} \in T[x] / (m)$ *maradékosztálynak akkor és csak akkor létezik multiplikatív inverze, ha* $\operatorname{lnko}(f, m) \sim 1$. *Ilyenkor a multiplikatív inverz egyértelműen meghatározott.*

Példa.

Határozzuk meg az $\overline{f} \in \mathbb{Z}_5[x] / (m)$ maradékosztály multiplikatív inverzét, ahol

$$f = x^2 + \overline{3}x + \overline{1}, \qquad m = x^3 + \overline{2}x^2 + \overline{4}x + \overline{2}.$$

$$\begin{aligned} \overline{u} \text{ inverze } \overline{f}\text{-nak} &\iff \overline{f} \cdot \overline{u} = \overline{\overline{1}} \\ &\iff f \cdot u \equiv \overline{1} \pmod{m} \\ &\iff u \equiv x^2 + \overline{4}x + \overline{1} \pmod{m} \end{aligned}$$

Tehát $\overline{f}$ multiplikatív inverze: $\overline{x^2 + \overline{4}x + \overline{1}}$.

Polinomfüggvény

3.17. Definíció.

Az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinom $c \in T$ helyen vett *helyettesítési értékén* az $f(c) = a_n c^n + \cdots + a_1 c + a_0 \in T$ elemet értjük.
Az $f \in T[x]$ polinomhoz tartozó *polinomfüggvény* pedig nem más, mint az

$$f : T \to T,\ c \mapsto f(c)$$

leképezés.

A polinomot és a hozzá tartozó polinomfüggvényt ugyanúgy jelöljük; a szövegkörnyezetből kiderül, hogy mikor melyikről van szó. Ha polinomfüggvényekről van szó, akkor x-et *változónak* nevezzük (nem pedig határozatlannak).

Polinom vs. polinomfüggvény

Példa.
Az $f = x^3 \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0}^3 = \overline{0},\ \overline{1} \mapsto \overline{1}^3 = \overline{1},\ \overline{2} \mapsto \overline{2}^3 = \overline{2}.$$

A $g = x \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0},\ \overline{1} \mapsto \overline{1},\ \overline{2} \mapsto \overline{2}.$$

Látjuk, hogy f-hez és g-hez ugyanaz a polinomfüggvény tartozik (nevezetesen az identikus függvény), noha f és g két különböző polinom. Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Polinom vs. polinomfüggvény

Általánosabban, ha T egy q-elemű test, akkor

- a $T \to T$ leképezések száma  q^q, míg
- T feletti polinomból  végtelen sok van,

így végtelen sok különböző polinomhoz tartozik ugyanaz a polinomfüggvény. Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Gyökök és oszthatóság

3.18. Definíció.

Az $\alpha \in T$ elem *gyök*e az $f \in T[x]$ polinomnak, ha $f(\alpha) = 0$.

3.19. Tétel (Bézout tétele).

Bármely $f \in T[x]$ *és* $\alpha \in T$ *esetén* $\quad f(\alpha) = 0 \iff x - \alpha \mid f$.

Bizonyítás.

Osszuk el f-et $(x - \alpha)$-val maradékosan:

$$f = q(x - \alpha) + r, \text{ ahol } q, r \in T[x] \text{ és } \deg r < \deg(x - \alpha) = 1.$$

Vegyük észre, hogy itt r konstans polinom. Értékeljük ki az $x = \alpha$ helyen a fenti egyenlőség mindkét oldalát:

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

Tehát

$$x - \alpha \mid f \iff r = 0 \iff f(\alpha) = 0.$$

□

Közös gyökök

3.20. Következmény.

Tetszőleges $f, g \in T[x]$ *polinomok esetén* f *és* g *közös gyökei ugyanazok, mint* $\operatorname{Inko}(f, g)$ *gyökei.*

Bizonyítás.

Legyen $d = \operatorname{Inko}(f, g)$. Tetszőleges $\alpha \in T$ esetén

$$\begin{aligned}
\alpha \text{ közös gyöke } f\text{-nek és } g\text{-nek} &\iff f(\alpha) = 0 \text{ és } g(\alpha) = 0 \\
&\iff x - \alpha \mid f \text{ és } x - \alpha \mid g \qquad \text{(Bézout)} \\
&\iff x - \alpha \mid d \qquad \text{(Inko def.)} \\
&\iff d(\alpha) = 0. \qquad \text{(tuozéB)}
\end{aligned}$$

□

Több gyöktényező kiemelése

3.21. Következmény.

Ha $\alpha_1, \ldots, \alpha_k \in T$ *páronként különböző elemek és* $f \in T[x]$, *akkor*

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f.$$

Bizonyítás.

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff x - \alpha_1, \ldots, x - \alpha_k \mid f \qquad \text{(Bézout)}$$

$$\iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \qquad \text{(miért?)}$$

□

A gyökök száma

3.22. Következmény.

Ha az $0 \neq f \in T[x]$ *polinom fokszáma* n*, akkor legfeljebb* n *különböző gyöke van a* T *testben.*

Bizonyítás.

Legyenek $\alpha_1, \ldots, \alpha_k \in T$ az f polinom összes különböző gyökei. Ekkor

$$(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \implies k \leq \deg f = n. \qquad \square$$

Megjegyzés.

Ha nem *test* feletti polinomokat tekintünk, akkor a gyökök száma meghaladhatja a fokszámot!

Például az $x^2 - \overline{1} \in \mathbb{Z}_{12}[x]$ polinomnak négy gyöke is van! 

Polinom vs. polinomfüggvény

3.23. Következmény.

Ha az $f, g \in T[x]$ polinomok legfeljebb n-edfokúak, és $n+1$ különböző helyen ugyanaz a helyettesítési értékük, akkor $f = g$.

3.24. Következmény.

Ha a T test végtelen, akkor két T feletti polinom akkor és csak akkor egyenlő, ha a hozzájuk tartozó polinomfüggvények megegyeznek.

3.25. Megjegyzés.

Ha a T test véges, akkor találhatók különböző T feletti polinomok, amelyekhez ugyanaz a polinomfüggvény tartozik (keressünk végtelen sok ilyen példát!). Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Lagrange-interpoláció

3.26. Tétel (Lagrange-interpoláció).

Tetszőleges $c_1, \ldots, c_{n+1}$ *páronként különböző és* $d_1, \ldots, d_{n+1}$ (*nem feltétlenül különböző*) T*-beli elemekhez létezik pontosan egy* $f \in T[x]$ *legfeljebb* n*-edfokú polinom, amelyre* $f(c_i) = d_i \ \ (i = 1, \ldots, n+1)$ *teljesül.*

3.27. Definíció.

Az előző tételbeli f polinom neve *Lagrange-féle interpolációs polinom*.

3.28. Megjegyzés.

Előfordulhat, hogy az $n+1$ pontra illesztett Lagrange-féle interpolációs polinom foka kisebb, mint n. Pontosan n-edfokú polinom létezését nem lehet garantálni. Ha nem kötünk ki semmit a fokszámra, akkor elveszítjük az unicitást: bármely $g \in T[x]$ polinomra $f + (x - c_1) \cdots (x - c_{n+1}) \cdot g$ is megfelelő. Nem nehéz meggondolni (tegyük meg!), hogy minden olyan polinom, amely a c_i helyeken a d_i értékeket veszi fel, előáll ilyen alakban.