Algebra és számelmélet előadás

Waldhauser Tamás
2016. október 6.

Asszociáltság

3.2. Definíció.

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

3.3. Tétel.

A $T[x]$ polinomgyűrűn az oszthatóság reflexív és tranzitív reláció, továbbá tetszőleges $f, g \in T[x]$ polinomokra

(1) $f \sim g \iff \exists c \in T \setminus \{0\} : g = cf$;

(2) $f \mid g$ és $g \neq 0 \implies \deg f \leq \deg g$.

3.4. Tétel.

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

Az oszthatóság szerinti részbenrendezés

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 $0/\sim = \{0\}$.

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

Maradékos osztás

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 $\deg r < \deg g$. Ebben a maradékos osztásban f az *osztandó*, g az *osztó*, q a *hányados* és r a *maradék*.

Példa.

Végezzünk maradékos osztást az alábbi $\mathbb{Z}_7$ feletti polinomokon:

$$f = \overline{3}x^5 + \overline{5}x^4 + \overline{5}x^3 + \overline{4}x^2 + \overline{3}x + \overline{1}, \qquad g = \overline{5}x^3 + x^2 + \overline{5}x + \overline{1}.$$

$$\begin{array}{l} (\overline{3}x^5 + \overline{5}x^4 + \overline{5}x^3 + \overline{4}x^2 + \overline{3}x + \overline{1}) \;:\; (\overline{5}x^3 + x^2 + \overline{5}x + \overline{1}) = \overline{2}x^2 + \overline{2}x \\ \underline{\overline{3}x^5 + \overline{2}x^4 + \overline{3}x^3 + \overline{2}x^2} \\ \qquad \overline{3}x^4 + \overline{2}x^3 + \overline{2}x^2 + \overline{3}x + \overline{1} \\ \qquad \underline{\overline{3}x^4 + \overline{2}x^3 + \overline{3}x^2 + \overline{2}x} \\ \qquad\qquad \overline{6}x^2 + x + \overline{1} \end{array}$$

A hányados: $q = \overline{2}x^2 + \overline{2}x$; a maradék: $\overline{6}x^2 + x + \overline{1}$.

Legnagyobb közös osztó

3.6. Definíció.

A $d \in T[x]$ polinom *legnagyobb közös osztója* 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 többszöröse* is.

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 d 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 3.3. Tételbeli (2) 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": $\exists u, v \in T[x]: \ fu + gv = \text{lnko}(f, g)$.

Példa.

Oldja meg az $fu + gv = \text{lnko}(f, g)$ egyenletet az $\mathbb{R}[x]$ polinomgyűrűben:

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

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

Tehát $\text{lnko}(f, g) \sim 2x^2 + 4x + 6 \sim x^2 + 2x + 3$.
Hab a tortán:

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

Példa (folyt.).

Az euklideszi algoritmus tömörebben összefoglalva:

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

Tehát $\operatorname{lnko}(f,g) \sim 2x^2+4x+6 \sim x^2+2x+3$.

Fejezzük ki a legnagyobb közös osztót f és g segítségével:

$$x^2+2x+3 = \frac{1}{2}\left(f-(x+1)\cdot g\right) = \frac{1}{2}\cdot f + \left(-\frac{1}{2}x-\frac{1}{2}\right)\cdot g$$

Az egyenlet egy megoldása: $u_0 = \frac{1}{2}, \quad v_0 = -\frac{1}{2}x-\frac{1}{2}$.

Diofantoszi egyenlet polinomgyűrűben

Példa.

Oldja meg az $fu + gv = \text{lnko}\,(f, g)$ egyenletet a $\mathbb{Z}_7\,[x]$ polinomgyűrűben:

$$f = x^6 + \overline{6}, \qquad g = x^4 + \overline{5}x + \overline{1} \in \mathbb{Z}_7\,[x]$$

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

Tehát $\text{lnko}\,(f, g) \sim \overline{2}x^2 + \overline{2}x + \overline{3} \sim x^2 + x + \overline{5}$.

Fejezzük ki a legnagyobb közös osztót f és g segítségével:

$$\begin{aligned} x^2 + x + \overline{5} = \overline{2}^{-1} \cdot \left(\overline{2}x^2 + \overline{2}x + \overline{3}\right) &= \overline{4} \cdot \left(g - \left(\overline{4}x + \overline{2}\right) \cdot \left(\overline{2}x^3 + \overline{6}x^2 + \overline{6}\right)\right) \\ &= \overline{4} \cdot \left(g - \left(\overline{4}x + \overline{2}\right) \cdot \left(f - x^2 \cdot g\right)\right) \\ &= \left(\overline{5}x + \overline{6}\right) \cdot f + \left(\overline{2}x^3 + x^2 + \overline{4}\right) \cdot g \end{aligned}$$

Az egyenlet egy megoldása: $u_0 = \overline{5}x + \overline{6}, \quad v_0 = \overline{2}x^3 + x^2 + \overline{4}$.

Diofantoszi egyenlet polinomgyűrűben

3.8. 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 $\text{lnko}(f, g) \mid h$.

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:

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

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

Kongruenciareláció

3.9. Definíció.

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

3.10. 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

3.11. Tétel.

Tetszőleges $f, g, h \in T[x]$ esetén az $fu \equiv h \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg (az u ismeretlen polinomra nézve), ha $\operatorname{lnko}(f, m) \mid h$.

Példa.

Oldja 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: $u_0 = x^2 + \overline{4}x + \overline{1}$ (és $v_0 = \overline{4}x$).

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

Lineáris kongruencia

Példa.

Oldja meg az $f \cdot u \equiv \overline{1} \pmod{m}$ konruenciát a $\mathbb{Z}_2[x]$ polinomgyűrűben, ahol

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

A szokásos módszer:

$$\begin{aligned} f \cdot u \equiv \overline{1} \pmod{m} \quad &\iff \quad \exists v \in \mathbb{Z}_2[x] : \ fu = \overline{1} + mv \\ &\iff \quad \exists v \in \mathbb{Z}_2[x] : \ fu - mv = \overline{1} \end{aligned}$$

$\ldots$ $u_0 = x^2 + x + \overline{1}$. Tehát a kongruencia megoldása: $u \equiv x^2 + x + \overline{1} \pmod{m}$.

Egy másik gondolatmenet:

$$\begin{aligned} f \cdot u \equiv \overline{1} \pmod{m} \quad &\iff \quad \left(x + \overline{1}\right)^2 \cdot u \equiv x^3 + x^2 \pmod{x^3 + x^2 + \overline{1}} \\ &\iff \quad \left(x + \overline{1}\right) \cdot u \equiv x^2 \pmod{x^3 + x^2 + \overline{1}} \\ &\iff \quad \left(x + \overline{1}\right) \cdot u \equiv x^3 + \overline{1} \pmod{x^3 + x^2 + \overline{1}} \\ &\iff \quad u \equiv x^2 + x + \overline{1} \pmod{x^3 + x^2 + \overline{1}} \end{aligned}$$

Házi feladat a gyakorlatra

13. feladat. Oldja meg az $f \cdot u \equiv \overline{1} \pmod{m}$ konruenciát.

(a) $f = x^2 + \overline{3}x + \overline{1},\ m = x^3 + \overline{2}x^2 + \overline{4}x + \overline{2} \in \mathbb{Z}_5[x]$

$u \equiv x^2 + \overline{4}x + \overline{1} \pmod{m}$

(b) $f = x^2 + \overline{1},\ m = x^3 + x^2 + \overline{1} \in \mathbb{Z}_2[x]$

$u \equiv x^2 + x + \overline{1} \pmod{m}$

(c) $f = \overline{3}x^2 + \overline{2},\ m = x^3 + x + \overline{1} \in \mathbb{Z}_5[x]$

(d) $f = \overline{2}x^2 + \overline{4},\ m = x^3 + x^2 + x + \overline{1} \in \mathbb{Z}_5[x]$

(e) $f = x^2,\ m = x^3 + x^2 + \overline{1} \in \mathbb{Z}_2[x]$

Maradékosztály-gyűrű

3.12. Definíció.

A mod m kongruenciához tartozó ekvivalenciaosztályokat modulo m *maradékosztályoknak* 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 $T[x]/(m) = \{\overline{f} : f \in T[x]\}$.

3.13. 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

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

3.14. Állítás.

A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (addditív 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

3.15. 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.

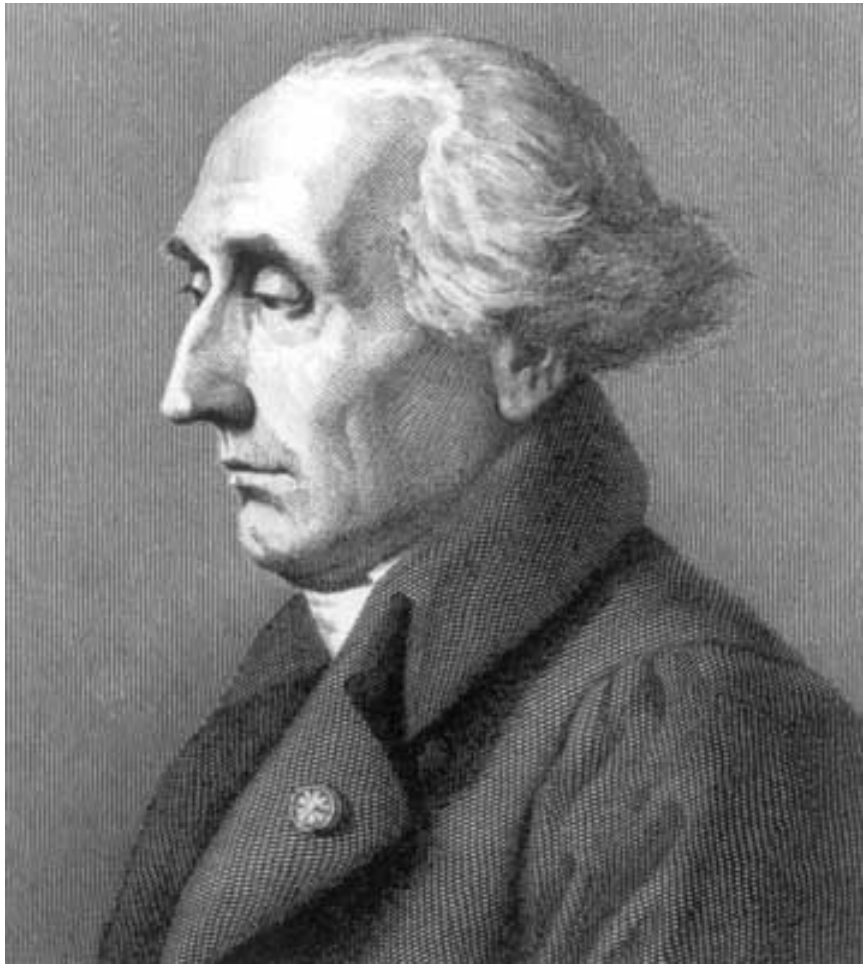
Határozza meg az $\overline{f} \in \mathbb{Z}_5[x] / (m)$ maradékosztály multiplikatív inverzét, ahol

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

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

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

Polinomfüggvények, gyökök, interpoláció



Joseph-Louis Lagrange

(1736, Torino – 1813, Párizs)

Polinomfüggvény

3.16. 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

3.17. Definíció.

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

3.18. Tétel (Bézout tétele).

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

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

3.19. Következmény.

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

Bizonyítás.

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

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

□

Több gyöktényező kiemelése

3.20. 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.

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

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

□

Horner-elrendezés

3.21. Definíció.

Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem *k-szoros gyöke*, ha $(x-\alpha)^k \mid f$ de $(x-\alpha)^{k+1} \nmid f$. A k számot az α gyök *multiplicitásának* nevezzük.

3.22. Megjegyzés.

Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ egy n-edfokú polinom és $c \in T$. Ha $f(c)$ értékét szereténk kiszámítani, akkor a szokásos $f(c) = a_n c^n + \cdots + a_1 c + a_0$ felírást használva $2n-1$ szorzást és n összeadást kell elvégeznünk. Ha viszont a disztributivitást kihasználva $f(c)$-t a következő alakban írjuk fel, akkor csak n szorzást és n összeadást kell elvégezni:

$$f(c) = ((\cdots(((a_n \cdot c + a_{n-1}) \cdot c + a_{n-2}) \cdot c + a_{n-3}) \cdots + a_2) \cdot c + a_1) \cdot c + a_0.$$

Ezt nevezzük *Horner-elrendezésnek*. Figyeljük meg, hogy balról jobbra haladva elvégezve a műveleteket a következő részeredmény mindig úgy adódik, hogy az előzőt megszorozzuk c-vel, és hozzáadjuk f soron következő együtthatóját. (Itt részeredményen az egy zárójelpáron belüli kifejezéseket értjük.)

Horner-módszer

A számolást kényelmesebb az alábbi táblázatban elvégezni.

	a_n	a_{n-1}	$\cdots$	$\diamondsuit$	$\spadesuit$	$\cdots$	a_0
c	a_n	$a_n \cdot c + a_{n-1}$	$\cdots$	$\clubsuit$	$\clubsuit \cdot c + \spadesuit$	$\cdots$	$f(c)$

Amint a következő tételből és következményéből kiderül, a Horner-elrendezés valójában nem csak $f(c)$ kiszámítására alkalmas.

Tétel (Horner-módszer).

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ egy n-edfokú polinom és $c \in T$. Ha a Horner-módszerrel elkészített táblázat alsó sorában álló elemek $b_n, \ldots, b_1, b_0$, azaz $b_n = a_n$ és $b_i = b_{i+1} \cdot c + a_i \ \ (i = n-1, \ldots, 0)$, akkor b_0 nem más, mint az f-nek az $x - c$ polinommal való osztásakor keletkező maradék, $b_n x^{n-1} + \cdots + b_2 x + b_1$ pedig ugyanezen osztás hányadosa:

$$f = (x - c) \cdot \left(b_n x^{n-1} + \cdots + b_2 x + b_1\right) + b_0.$$

Házi feladat a gyakorlatra

14. feladat. A Horner-módszer segítségével határozza meg az f polinom c gyökének multiplicitását.

(a) $f = x^3 - 4x^2 + 5x - 2,\ c = 1$

kétszeres gyök, $f = (x-1)^2(x-2)$

(b) $f = x^6 + 4x^5 + 7x^4 + 8x^3 + 7x^2 + 4x + 1,\ c = -1$

négyszeres gyök, $f = (x+1)^4(x^2+1)$

(c) $f = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8,\ c = 2$

(d) $f = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16,\ c = -2$

(e) $f = x^3 + x^2 + x + 1,\ c = i$

Iterált Horner-módszer

Következmény (iterált Horner-módszer).

Alkalmazzuk a Horner-módszert az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinomra és a $c \in T$ elemre, majd egészítsük ki a táblázatot egy újabb, az előzőnél eggyel rövidebb sorral a fentebb leírt számolási szabályt követve. Folytassuk újabb, egyre rövidebb sorokkal, míg végül egy háromszög alakú táblázatot kapunk:

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c			$\cdots$		d_0
c			$\cdots$	d_1	
$\vdots$	$\vdots$	$\vdots$	$\iddots$		
c		d_{n-1}			
c	d_n				

A táblázat jobb szélén átlósan elhelyezkedő elemek megadják annak a polinomnak az együtthatóit, amelyet f-ből az $x - c$ határozatlanra való áttéréssel kapunk:

$$a_n x^n + \cdots + a_1 x + a_0 = d_n (x - c)^n + \cdots + d_1 (x - c) + d_0.$$

Ha $d_0 = \cdots = d_{k-1} = 0$ és $d_k \neq 0$, akkor a $c \in T$ elem k-szoros gyöke f-nek.

Házi feladat a gyakorlatra

15. feladat. Döntse el, hogy igazak-e az alábbi állítások. A választ minden esetben indokolni kell!

(a) Minden $f, g \in \mathbb{Z}_3[x]$ esetén, ha $f \mid g$ és $g \mid f$, akkor $f = g$.

Hamis; egy ellenpélda: $f = x,\ g = -x$

(b) Létezik olyan $f \in \mathbb{Z}_2[x]$ polinom, amelynek végtelen sok osztója van.

Igaz, pl. $f = 0$ (más ilyen példa nincs is!).

(c) Minden $f, g \in \mathbb{Z}_2[x]$ esetén, ha $f \mid g$ és $g \mid f$, akkor $f = g$.

(d) Léteznek olyan $f \neq g \in \mathbb{Z}_3[x]$ polinomok, melyekre minden $c \in \mathbb{Z}_3$ esetén $f(c) = g(c)$.

(e) Létezik olyan $f \in \mathbb{R}[x]$ polinom, amelyre $\operatorname{lnko}(f, x^3 - 1) = x + 1$.