Algebra és számelmélet előadás

Waldhauser Tamás
2016. szeptember 29.


...THEY HAD TO CUT DOWN ALL THE TREES TO PRINT ALL THE BAILOUT MONEY NEEDED TO CREATE GREEN JOBS TO SAVE THE ENVIRONMENT...

Házi feladat a gyakorlatra

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

(a) Létezik olyan gyűrű, ami egységelemes, de nem kommutatív és nem zérusosztómentes.

Igaz, pl. $\mathbb{R}^{2\times 2}$.

(b) Létezik olyan integritástartomány, amelyben pontosan tizenhat egység van.

Igaz, pl. $\mathbb{Z}_{17}$.

(c) Az egységek minden gyűrűben csoportot alkotnak az összeadás műveletével.

(d) Létezik olyan gyűrű, ami kommutatív és egységelemes, de nem integritástartomány.

(e) Létezik olyan integritástartomány, amelyben csak véges sok egység van.

A polinom definíciója

2.18. Definíció.

Az R integritástartomány feletti *polinomnak* 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 *együtthatóinak* nevezzük. Az R feletti polinomok halmazát $R[x]$ jelöli.

2.19. Definíció.

- Az $f = (a_0, a_1, \ldots)$ polinom *fokszámán* 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 $-\infty$. Az f polinom fokszámát $\deg f$ jelöli.
- 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 *főegyütthatójának* hívjuk.
- Az olyan polinomot, amelynek főegyütthatója 1, *főpolinomnak* nevezzük.

Műveletek polinomokkal

2.20. Definíció.

Az $f = (a_0, a_1, \ldots)$ és $g = (b_0, b_1, \ldots)$ polinomok *összegét* és *szorzatát* az alábbi képletekkel értelmezzük:

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

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

2.21. Állítás.

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

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

2.22. Tétel.

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

2.23. Definíció.

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

Az alapgyűrű beágyazása

2.24. Állítás.

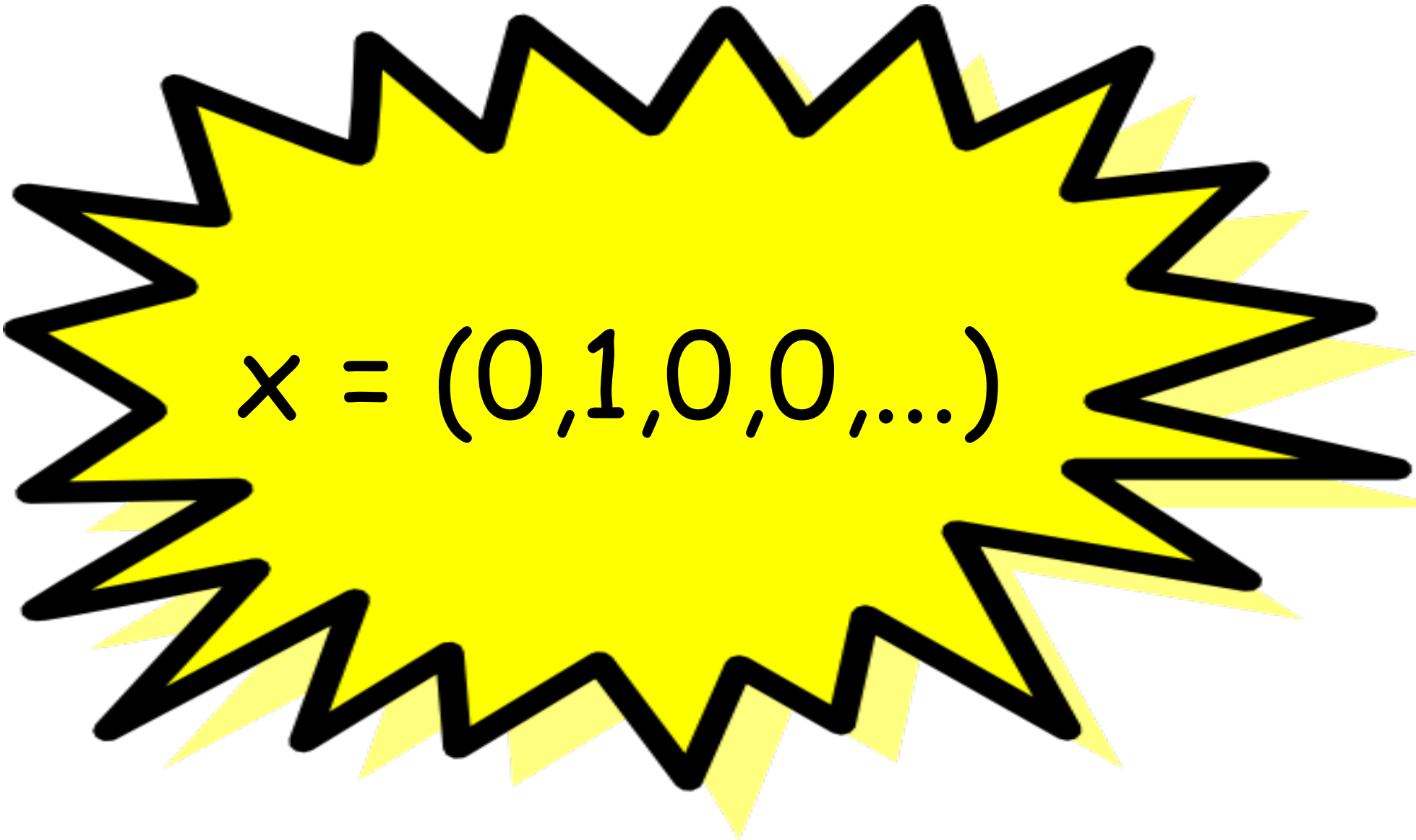
Minden $a, b \in R$ esetén

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

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

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 $R \subseteq R[x]$.)


x = (0,1,0,0,...)

Kanonikus alak

2.24. 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.

2.25. Tétel.

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

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

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 $R[y]$.)

2.26. 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

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

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.

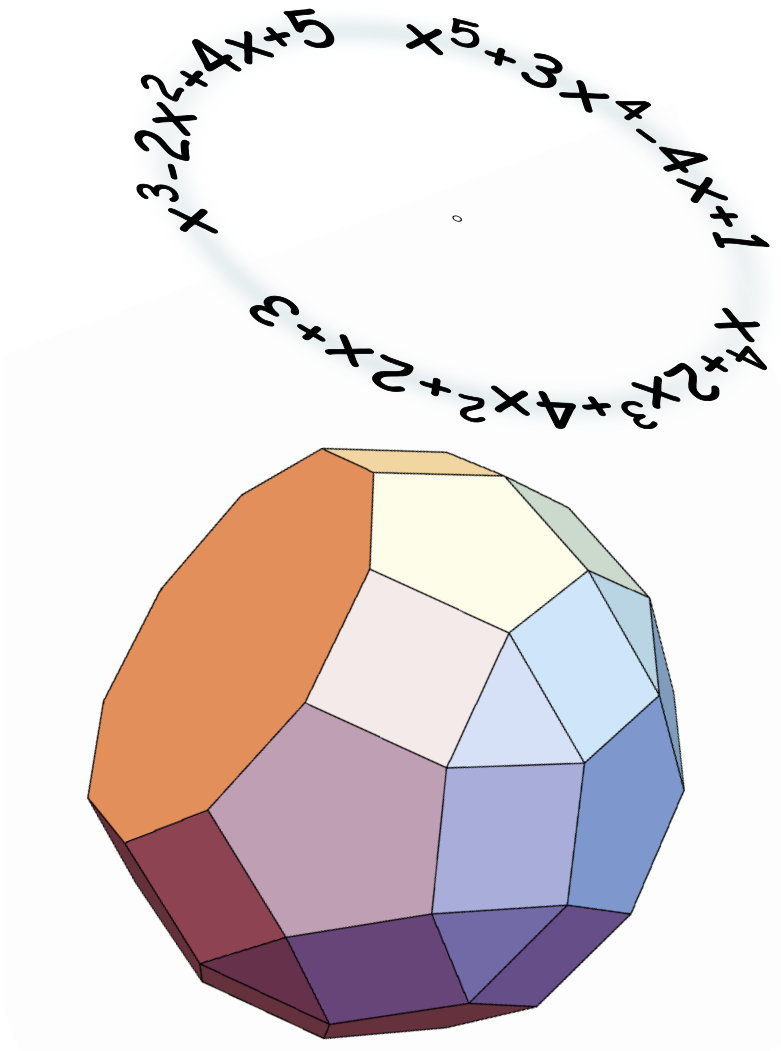
Tekintsük $\mathbb{Z}_2$ felett az $f = x$ és $g = x^{2016}$ polinomokat. Ez nyilván két különböző polinom (még a fokszámuk is különbözik), de ugyanaz a polinomfüggvény tartozik hozzájuk:

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

$$g\colon \{\overline{0}, \overline{1}\} \to \{\overline{0}, \overline{1}\},\quad \overline{0} \mapsto \overline{0}^{2016},\quad \overline{1} \mapsto \overline{1}^{2016}.$$

3. Test feletti egyhatározatlanú polinomok

A polinomok számelmélete



Paragyrate Diminished Rhombicosidodecahedron

Oszthatóság test feletti polinomok körében

3.1. Definíció.

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

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) $1 \mid f$;

(4) $f \mid 0$;

(5) $(f \mid g \text{ és } f \mid h) \implies f \mid g + h$.

Oszthatóság az egész számok körében

Definíció.

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

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) $1 \mid a$;

(4) $a \mid 0$;

(5) $(a \mid b \text{ és } a \mid c) \implies a \mid b + c$.

Negyedik házi feladat az előadásra

Legyen R egy tetszőleges integritástartomány. Definiáljuk az oszthatósági relációt R-en a következőképpen: $a \mid b \iff \exists c \in R\colon b = ac$.

Bizonyítsa be, hogy az oszthatósági reláció rendelkezik az alábbi tulajdonságokkal:

(1) $\forall a \in R\colon a \mid a$;

(2) $\forall a, b, c \in R\colon (a \mid b \text{ és } b \mid c) \implies a \mid c$;

(3) $\forall a \in R\colon 1 \mid a$;

(4) $\forall a \in R\colon a \mid 0$;

(5) $\forall a, b, c \in R\colon (a \mid b \text{ és } a \mid c) \implies a \mid b + c$.

Mindig mutasson rá, hogy az integritástartomány definíciójának pontosan melyik részét használja éppen.

- beküldendő emailben: `twaldha@math.u-szeged.hu`
- pdf fájl legyen (lehet szkennelt is)
- fájlnév: `EHA-eahf4.pdf` (például `WATHAAS-eahf4.pdf`)
- határidő: október 12, reggel 8 óra

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:

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

Diofantoszi egyenlet polinomgyűrűben

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

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

Házi feladat a gyakorlatra

11. feladat. Számítsa ki az f és g polinomok legnagyobb közös osztóját.

(a) $f = x^4 + 2x^3 + 4x^2 + 2x + 3,\ g = x^3 + x^2 + x - 3 \in \mathbb{R}[x]$

$\text{Inko}(f, g) \sim x^2 + 2x + 3$

(b) $f = x^4 + x^3 + x,\ g = x^4 + x^2 + x \in \mathbb{Z}_2[x]$

$\text{Inko}(f, g) \sim x$

(c) $f = x^4 + 2x^3 - x^2 - 4x - 2,\ g = x^4 + x^3 - x^2 - 2x - 2 \in \mathbb{R}[x]$

(d) $f = x^4 + x^3 + 2x^2 + 3x - 3,\ g = x^4 + x^3 + x^2 + 3x - 6 \in \mathbb{Q}[x]$

(e) $f = x^4 + x^3 + x^2 + \overline{1},\ g = x^3 + \overline{1} \in \mathbb{Z}_2[x]$

Házi feladat a gyakorlatra

12. feladat. Oldja meg az $fu + gv = \text{lnko}(f, g)$ egyenletet.

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

$\text{lnko}(f, g) \sim x^2 + x + \overline{5},\ u = \overline{5}x + \overline{6},\ v = \overline{2}x^3 + x^2 + \overline{4}$

(b) $f = x^8 - 3x + 2,\ g = x^6 - x^5 + 3x - 2 \in \mathbb{R}[x]$

$\text{lnko}(f, g) \sim x^3 + x - 1,$

$u = \frac{1}{32}\left(-3x^2 + x - 7\right),\ v = \frac{1}{32}\left(3x^4 + 2x^3 + 9x^2 + 9x + 9\right)$

(c) $f = x^5 + x + \overline{2},\ g = x^4 + \overline{2}x^2 + \overline{2}x + \overline{1} \in \mathbb{Z}_3[x]$

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

(e) $f = x^5 + 3x^4 + 6x^3 + 6x^2 + 4x + 1,\ g = x^3 + 4x^2 + 4x + 3 \in \mathbb{R}[x]$