

Diszkrét matematika 2.

Szoftvertervező szakirány
Polinomok

Juhász Zsófia

jzsofi@gmail.com, jzsofia@compalg.inf.elte.hu

Mérai László diái alapján

Komputeralgebra Tanszék

2019. ősz

Műveletek

Definíció (művelet)

Egy X halmazon értelmezett (r -változós, „ r -ér”) **művelet** alatt egy $* : X^r \rightarrow X$ függvényt értünk.

Egy X halmazon értelmezett **binér** (kétváltozós) **művelet** egy $* : X \times X \rightarrow X$ függvény. Gyakran $*(x, y)$ helyett $x * y$ -t írunk.

Egy X halmazon értelmezett **unér** (egyváltozós) **művelet** egy $* : X \rightarrow X$ függvény.

Példa

- \mathbb{C} halmazon az $+$ is, és \cdot is **binér műveletek**.
- \mathbb{C} halmazon az \div (osztás) **nem művelet**, mert $\text{dmn}(\div) \neq \mathbb{C} \times \mathbb{C}$.
- $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ halmazon az \div **binér művelet**.
- \mathbb{C} halmazon a 0 illetve 1 konstans kijelölése **nullér művelet**.
- \mathbb{R}^n ($n > 1$) vektortéren a vektorok skaláris szorzása **nem művelet**, mert $\text{rng}(\langle, \rangle) = \mathbb{R} \neq \mathbb{R}^n$ (a szorzás eredménye **nem** vektor)
- \mathbb{R}^n vektortéren egy adott $\lambda \in \mathbb{R}$ skalárral **való** szorzás **unér művelet**

Algebrai struktúrák

Definíció (algebrai struktúra)

A $(H; M)$ pár **algebrai struktúra**, ha H egy halmaz, M pedig H -n értelmezett műveletek halmaza.

A $(H; \{*, +, \circ\})$ jelölés helyett a $(H; *, +, \circ)$ jelölést is használhatjuk.

Definíció (grupoid)

Ha az M művelethalmaz **egyetlen műveletet** tartalmaz, és az egy **binér művelet**, akkor a $(H; M)$ struktúrát **grupoidnak** nevezzük.

- $(\mathbb{N}; +)$ algebrai struktúra, mert természetes számok összege természetes szám, és grupoid is.
- $(\mathbb{N}; -)$ **nem** algebrai struktúra, mert például $0 - 1 = -1 \notin \mathbb{N}$.
- $(\mathbb{Z}; +, \cdot)$ algebrai struktúra, mert egész számok összege és szorzata egész szám, de **nem** grupoid, de **nem** grupoid, mert **két művelet** van.
- $(\mathbb{C}; +, \cdot)$ algebrai struktúra, mert komplex számok összege és szorzata komplex szám, de **nem** grupoid, mert **két művelet** van.

Félcsoportok

Definíció (félcsoport)

A $(G; *)$ grupoid **félcsoport**, ha $*$ **asszociatív** G -n, azaz, ha:

$$\forall a, b, c \in G : (a * b) * c = a * (b * c).$$

Definíció (egységelem/semleges elem, monoid)

Ha a $(G; *)$ **félcsoportban** létezik olyan $s \in G$ elem, amelyre $\forall g \in G : s * g = g * s = g$, akkor az s elemet **semleges elemnek** (más néven **egységelemnek**) nevezzük.

Ekkor $(G; *)$ **semleges elemes félcsoport**, **egységelemes félcsoport**, más néven **monoid**.

- \mathbb{N} az $+$ művelettel egységelemes félcsoport a 0 egységelemmel.
- \mathbb{Q} a \cdot művelettel egységelemes félcsoport az 1 egységelemmel.
- $\mathbb{C}^{k \times k}$ a mátrixszorzással egységelemes félcsoport az egységmátrixszal mint egységelemmel.

Csoportok

Definíció (elem inverze)

Legyen $(G; *)$ egy egységelemes félcsoport e egységelemmel. A $g \in G$ elem **inverze** az a $g^{-1} \in G$ elem, melyre $g * g^{-1} = g^{-1} * g = e$.

Egy elemnek nem feltétlenül létezik inverze, de ha létezik, akkor egyértelmű. (Miért is? Kell hozzá a művelet **asszociativitása**!)

Definíció (csoport)

Ha a $(G; *)$ egy egységelemes félcsoportban minden $g \in G$ elemnek létezik inverze, akkor $(G; *)$ **csoport**.

Definíció (Abel-csoport)

Ha a $(G; *)$ csoportban a $*$ csoportművelet **kommutatív**, akkor $(G; *)$ **Abel-csoport**.

Csoportok

Példák csoportokra:

- $(\mathbb{Z}; +)$, $(\mathbb{Q}; +)$, $(\mathbb{R}; +)$ és $(\mathbb{C}; +)$ a 0 egységelemmel Abel-csoportok.
- $(\mathbb{Q}^*; \cdot)$, $(\mathbb{R}^*; \cdot)$ és $(\mathbb{C}^*; \cdot)$ az 1 egységelemmel Abel-csoportok, ahol $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ és $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.
- $\{M \in \mathbb{C}^{k \times k} : \det M \neq 0\}$ a mátrixszorzással, és az egységmátrixszal mint egységelemmel, csoport (de $k > 1$ esetén nem Abel).
- $X \rightarrow X$ bijektív függvények a kompozícióval, az $id_X : x \mapsto x$ identikus leképzéssel mint egységelemmel csoport, de nem Abel-csoport.

Gyűrűk

Definíció (disztributivitás)

Legyen $(R; \oplus, \otimes)$ algebrai struktúra, ahol \oplus és \otimes binér műveletek. Azt mondjuk, hogy teljesül a \otimes -nak a \oplus -ra vonatkozó **bal oldali disztributivitása**, illetve **jobb oldali disztributivitása**, ha

$\forall k, l, m \in R$ -re: $k \otimes (l \oplus m) = (k \otimes l) \oplus (k \otimes m)$, illetve

$\forall k, l, m \in R$ -re: $(l \oplus m) \otimes k = (l \otimes k) \oplus (m \otimes k)$.

Példa

$(\mathbb{Z}; +, \cdot)$ esetén teljesül a szorzás összeadásra vonatkozó mindkét oldali disztributivitása.

Szokásos elnevezések, bevett jelölések

$(R; \oplus, \otimes)$ két binér műveletes algebrai struktúra esetén szokás az \oplus műveletet „összeadásnak” és a \otimes műveletet „szorzásnak” nevezni (ha nem okoz félreértést). Az \oplus -ra vonatkozó semleges elemet ekkor **nullelemnek**, a \otimes -ra vonatkozó semleges elemet **egységelemnek** nevezzük. A nullelem szokásos jelölése **0**, az egységelemé **1**, esetleg **e**.

Gyűrűk

Definíció (gyűrű)

Az $(R; \oplus, \otimes)$ két binér műveletes algebrai struktúra **gyűrű**, ha

- $(R; \oplus)$ **Abel-csoport** (kommutatív csoport a 0 egységelemmel);
- $(R; \otimes)$ **félcsoport**;
- teljesül a \otimes -nak a \oplus -ra vonatkozó **mindkét oldali disztributivitása**.

$(R; \oplus, \otimes)$ gyűrű 0 nulleleme tehát $(R; \oplus)$ Abel-csoport egységeleme.

Példa: $(\mathbb{Z}, +, \cdot)$ gyűrű.

Állítás (Nullelemmel való szorzás gyűrűben)

Legyen $(R; \oplus, \otimes)$ gyűrű $0 \in R$ nullelemmel. Ekkor $\forall r \in R$ esetén $0 \otimes r = r \otimes 0 = 0$.

Bizonyítás

$$0 \otimes r = (0 \oplus 0) \otimes r = (0 \otimes r) \oplus (0 \otimes r) \implies 0 = 0 \otimes r.$$

A másik állítás bizonyítása ugyanígy.

Gyűrűk

Definíció (egységelemes gyűrű)

Az $(R; \oplus, \otimes)$ gyűrű **egységelemes gyűrű**, ha R -en a \otimes műveletre nézve **is** van egységelem: **1** vagy **e**. Azaz ha $(R; \otimes)$ **egységelemes félcsop.**

Definíció (kommutatív gyűrű)

Az $(R; \oplus, \otimes)$ gyűrű **kommutatív gyűrű**, ha a \otimes művelet **is** kommutatív. Azaz ha $(R; \otimes)$ **kommutatív félcsop.**

Példa

- $(\mathbb{Z}; +, \cdot)$ egységelemes kommutatív gyűrű.
- $(2\mathbb{Z}; +, \cdot)$ kommutatív gyűrű, de **nem** egységelemes.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a szokásos műveletekkel egységelemes kommutatív gyűrűk.
- $(\mathbb{Z}^{k \times k}, +, \cdot), (\mathbb{Q}^{k \times k}, +, \cdot), (\mathbb{R}^{k \times k}, +, \cdot)$ és $(\mathbb{C}^{k \times k}, +, \cdot)$ a szokásos mátrixösszeadással és mátrixszorzással egységelemes gyűrű, de **nem** kommutatív, ha $k > 1$.
- $(\mathbb{R}^3; +, \times)$ a 3-dim Euklideszi vektortér a vektoriális szorzással **NEM** gyűrű mert \times **nem** asszociatív, ezért $(\mathbb{R}^3; \times)$ **nem** félcsop.

Nullosztómentes gyűrűk

Definíció (nullosztómentes gyűrű)

Ha egy legalább kételemű (R, \oplus, \otimes) gyűrűben $\forall r, s \in R, r \neq 0, s \neq 0$ esetén $r \otimes s \neq 0$, akkor R **nullosztómentes gyűrű**. (Ilyenkor $r \otimes s = 0 \Rightarrow r = 0$ vagy $s = 0$)

Példa

Nem nullosztómentes gyűrű

- $(\mathbb{R}^{2 \times 2}; +, \cdot)$:
$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Integritási tartományok

Definíció (integritási tartomány)

A **kommutatív**, **nullosztómentes** gyűrűt **integritási tartománynak** nevezzük.

Példa: $(\mathbb{Z}; +, \cdot)$

Definíció (oszthatóság egységelemes integritási tartományban)

Az $(R; \oplus, \otimes)$ egységelemes integritási tartományban az $a, b \in R$ elemekre azt mondjuk, hogy a **osztója** b -nek, ha van olyan $c \in R$, amire $b = a \otimes c$. Jelölése: $a|b$.

Definíció (egységek egységelemes integritási tartományban)

Egy egységelemes integritási tartomány egy olyan elemét, amely az integritási tartomány minden elemének osztója, **egységnek** nevezünk.

Ne keverjük az egység**elem** és az **egység** fogalmát! Az egységelem mindig egység is, de nem az egységelemen kívül lehetnek más egységek is.

Egységelemből csak egyetlen egy van (az **1** jelöli), egységből esetleg (tipikusan) több is.

Testek és ferdetestek

Definíció (ferdetest)

Az $(R; \oplus, \otimes)$ egységelemes gyűrű **ferdetest**, ha $(R \setminus \{0\}; \otimes)$ csoport.

Definíció (test)

A kommutatív ferdetestet (azaz amiben nemcsak az összeadás, hanem a szorzás is kommutatív) **testnek** nevezzük.

Példa: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a szokásos műveletekkel **testek**.

Állítás (Test nullosztómentes)

Test nullosztómentes.

Bizonyítás

Legyen $(F; \oplus, \otimes)$ test $0 \in F$ nullelemmel. Ekkor a definíció szerint $(F \setminus \{0\}; \otimes)$ csoport, azaz $F \setminus \{0\}$ zárt a \otimes műveletre, ahonnan az állítás következik.

A $\text{mod } m$ maradékosztályok \mathbb{Z}_m gyűrűje

Jelölés: Tetszőleges m egész esetén \mathbb{Z}_m jelöli a $\text{mod } m$ maradékosztályok halmazát.

A $\text{mod } m$ maradékosztályok között (azaz \mathbb{Z}_m elemein) természetes módon műveleteket definiálhatunk:

Definíció (maradékosztályok összeadása és szorzása)

Rögzített m modulus, és a, b egészek esetén legyen:

$$\bar{a} + \bar{b} \stackrel{\text{def}}{=} \overline{a + b}; \quad \bar{a} \cdot \bar{b} \stackrel{\text{def}}{=} \overline{a \cdot b}.$$

Állítás (A műveletek a maradékosztályokon jól definiáltak)

Ez értelmes definíció, azaz, ha $\bar{a} = \overline{a^}$, $\bar{b} = \overline{b^*}$, akkor $\bar{a} + \bar{b} = \overline{a^* + b^*}$, illetve $\bar{a} \cdot \bar{b} = \overline{a^* \cdot b^*}$.*

Bizonyítás

Mivel $\bar{a} = \overline{a^*}$, $\bar{b} = \overline{b^*} \Rightarrow a \equiv a^* \pmod{m}$, $b \equiv b^* \pmod{m} \Rightarrow$
 $\Rightarrow a + b \equiv a^* + b^* \pmod{m} \Rightarrow \overline{a + b} = \overline{a^* + b^*} \Rightarrow \bar{a} + \bar{b} = \overline{a^* + b^*}$.
Szorzás hasonlóan.



A $\text{mod } m$ maradékosztályok \mathbb{Z}_m gyűrűje

A maradékosztályok között természetes módon műveleteket definiálhatunk: $\overline{a} + \overline{b} = \overline{a + b}$; $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Példák

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

+	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

\cdot	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}.$$

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

\cdot	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A $\text{mod } m$ maradékosztályok \mathbb{Z}_m gyűrűje

Tétel (\mathbb{Z}_m egységelemes, kommutatív gyűrű)

Tetszőleges m egész esetén $(\mathbb{Z}_m, +, \cdot)$ – ahol $+$ és \cdot a maradékosztályok összeadását, ill. szorzását – egységelemes, kommutatív gyűrű.

Könnyen belátható, hogy ha m nem prímszám, akkor \mathbb{Z}_m nem nullosztómentes (tehát test sem lehet).

Tétel (\mathbb{Z}_p test)

Tetszőleges p prímszám esetén $(\mathbb{Z}_p, +, \cdot)$ test.

Nullosztómentes gyűrűk karakterisztikája

Jelölés: Tetszőleges R gyűrű, $a \in R$ és $n \in \mathbb{N}^+$ esetén legyen $na = \underbrace{a + a + \dots + a}_n$ (n tagú összeg, melynek minden tagja a).

Definíció (elem additív rendje gyűrűben)

Egy R gyűrű egy a elemének **additív rendje** a legkisebb olyan pozitív egész n , amelyre $na = 0$, ha ilyen n létezik. Egyébként a **additív rendje** végtelen.

Állítás (Elemek additív rendje nullosztómentes gyűrűben)

Nullosztómentes gyűrűben a nem-nulla elemek additív rendje megegyezik, és vagy egy p prímszám vagy végtelen.

Definíció (nullosztómentes gyűrű karakterisztikája)

Ha az előző állításban szereplő közös rend p , akkor azt mondjuk, hogy a gyűrű **karakterisztikája** p (jelölése: $\text{char}(R) = p$), ha pedig ez a közös rend végtelen, akkor a gyűrű karakterisztikája $\text{char}(R) = 0$.

Példák: $\text{char}(\mathbb{Z}) = \text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$; $\text{char}(\mathbb{Z}_p) = p$ (p prím)

Polinomok alapfogalmai

Definíció (polinom, polinomok összege és szorzata)

Legyen $(R; +, \cdot)$ gyűrű. A gyűrű elemeiből képzett $f = (f_0, f_1, f_2, \dots)$ ($f_j \in R$) végtelen sorozatot R fölötti **polinomnak** nevezzük, ha csak véges sok eleme nem-nulla.

Az R fölötti polinomok halmazát $R[x]$ -szel jelöljük.

$R[x]$ elemein definiáljuk az **összeadást** és a **szorzást**.

$f = (f_0, f_1, f_2, \dots)$, $g = (g_0, g_1, g_2, \dots)$ és $h = (h_0, h_1, h_2, \dots)$ esetén $f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \dots)$ és $f \cdot g = h$, ahol

$$h_k = \sum_{i+j=k} f_i g_j = \sum_{i=0}^k f_i g_{k-i} = \sum_{j=0}^k f_{k-j} g_j.$$

Két polinom pontosan akkor egyenlő, ha minden tagjuk egyenlő:

$$f = g \Leftrightarrow \forall j \in \mathbb{N} : f_j = g_j.$$

Megjegyzés

Könnyen látható, hogy polinomok összege és szorzata is polinom.

Polinomok alapfogalmai

Jelölés

Az $f = (f_0, f_1, f_2, \dots, f_n, 0, 0, \dots)$, $f_n \neq 0$ ($f_m = 0 : \forall m > n$) polinomot $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$, $f_n \neq 0$ alakba írjuk.

Definíció (polinom együtthatói, tagjai, foka)

Az előző pontban szereplő polinom esetén $f_i x^i$ a polinom i -ed fokú tagja, f_i -t az i -ed fokú tag együtthatójának nevezzük; f_0 a polinom konstans tagja, $f_n x^n$ a főtagja, f_n a főegyütthatója. A polinom foka n , melynek jelölésére $\deg(f)$ használatos.

Példa

Az $f = (1, 0, 2, 0, 0, 3, 0, \dots)$ polinom felírható $f(x) = 1 + 0x + 2x^2 + 0x^3 + 0x^4 + 3x^5$ alakban.

Ugyanezen f további alakjai:

$$f(x) = 1 + 2x^2 + 3x^5, \quad f(x) = 3x^5 + 2x^2 + 1.$$

Polinomok alapfogalmai

Megjegyzés

A főegyüttható tehát a legnagyobb indexű nem-nulla együttható, a fok pedig ennek indexe.

A $0 = (0, 0, \dots)$ **nullpolinomnak** nincs legnagyobb indexű nem-nulla együtthatója, így a fokát külön definiáljuk, mégpedig $\deg(0) = -\infty$.

Definíció (konstans polinomok, lineáris polinomok)

A **konstans polinomok** a legfeljebb nulladfokú polinomok, a **lineáris polinomok** pedig a legfeljebb elsőfokú polinomok. Az $f_i x^i$ alakba írható polinomok a **monomok**. Ha $f \in R[x]$ polinom főegyütthatója R egységeleme, akkor f -et **főpolinomnak** nevezzük.

Példa

- $x^3 + 1 \in \mathbb{Z}[x]$
- $\frac{2}{3} \in \mathbb{Q}[x]$
- $\pi x + (i + \sqrt{2}) \in \mathbb{C}[x]$

Polinomok alapfogalmai

Állítás (NB)

Ha $(R; +, \cdot)$ gyűrű, akkor $(R[x]; +, \cdot)$ is gyűrű, és R fölötti **polinomgyűrűnek** nevezzük.

Megjegyzés

Gyakran az $(R; +, \cdot)$ gyűrűre szimplán R -ként, az $(R[x]; +, \cdot)$ gyűrűre $R[x]$ -ként hivatkozunk.

Állítás (Kommutatív gyűrű feletti polinomgyűrű)

Ha az R gyűrű kommutatív, akkor $R[x]$ is kommutatív.

Bizonyítás

$$\begin{aligned}(f \cdot g)_k &= f_0 g_k + f_1 g_{k-1} + \dots + f_{k-1} g_1 + f_k g_0 = \\&= g_k f_0 + g_{k-1} f_1 + \dots + g_1 f_{k-1} + g_0 f_k = \\&= g_0 f_k + g_1 f_{k-1} + \dots + g_{k-1} f_1 + g_k f_0 = (g \cdot f)_k\end{aligned}$$

Polinomok alapfogalmai

Állítás (Egységelemes gyűrű feletti polinomgyűrű egységeleme)

$1 \in R$ egységelem esetén $e = (1, 0, 0 \dots)$ egységeleme lesz $R[x]$ -nek.

Bizonyítás

$$(f \cdot e)_k = \sum_{j=0}^k f_j e_{k-j} = \sum_{j=0}^{k-1} f_j e_{k-j} + f_k e_0 = f_k$$

Állítás (Nullosztómentes gyűrű feletti polinomgyűrű)

Ha az R gyűrű nullosztómentes, akkor $R[x]$ is nullosztómentes.

Bizonyítás

Legyen n , illetve m a legkisebb olyan index, amire $f_n \neq 0$, illetve $g_m \neq 0$.

$$\begin{aligned} (f \cdot g)_{n+m} &= \sum_{j=0}^{n+m} f_j g_{n+m-j} = \sum_{j=0}^{n-1} f_j g_{n+m-j} + f_n g_m + \sum_{j=n+1}^{n+m} f_j g_{n+m-j} = \\ &= 0 + f_n g_m + 0 = f_n g_m \neq 0 \end{aligned}$$

Alapfogalmak

Állítás (Polinomok összegének, ill. szorzatának foka)

Legyen $f, g \in R[x]$, $\deg(f) = n$, és $\deg(g) = k$. Ekkor:

- $\deg(f + g) \leq \max(n, k)$;
- $\deg(f \cdot g) \leq n + k$.

Bizonyítás

Legyen $h = f + g$. Ekkor $j > \max(n, k)$ esetén $h_j = 0 + 0 = 0$.

Legyen $h = f \cdot g$. Ekkor $j > n + k$ esetén

$$h_j = \sum_{i=0}^j f_i g_{j-i} = \sum_{i=0}^n f_i g_{j-i} + \sum_{i=n+1}^j f_i g_{j-i} = \sum_{i=0}^n f_i \cdot 0 + \sum_{i=n+1}^j 0 \cdot g_{j-i} = 0.$$

Polinomok alapfogalmai

Megjegyzés

Nullosztómentes gyűrű esetén egyenlőség teljesül a 2. egyenlőtlenségben, hiszen

$$h_{n+k} = \sum_{i=0}^{n+k} f_i g_{n+k-i} = \sum_{i=0}^{n-1} f_i g_{n+k-i} + f_n g_k + \sum_{i=n+1}^{n+k} f_i g_{n+k-i} = f_n g_k \neq 0.$$

Polinomok alapfogalmai

Definíció (helyettesítési érték)

Az $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n \in R[x]$ polinom $r \in R$ helyen felvett **helyettesítési értékén** az $f(r) = f_0 + f_1r + f_2r^2 + \dots + f_nr^n \in R$ elemet értjük.

Definíció (gyök)

$f(r) = 0$ esetén r -et a polinom **gyökének** nevezzük.

Példa $f(x) = x^2 + x - 2 \in \mathbb{Z}[x]$ -nek a -2 helyen felvett helyettesítési értéke $(-2)^2 + (-2) - 2 = 0$, ezért -2 gyöke f -nek.

Definíció (polinomfüggvény)

Az $\hat{f} : r \mapsto f(r)$ leképezés az f polinomhoz tartozó **polinomfüggvény**.

Másik tárgyban lehet, hogy az itt „polinomfüggvénynek” nevezett cuccot hívtátok „polinomnak”, és bizonyos esetekben ez nem is okoz gondot, de ebben a tárgyban gondosan ügyeljetek a két fogalom közötti különbségre!

Polinomok alapfogalmai

Megjegyzés

Ha R véges, akkor csak véges sok $R \rightarrow R$ függvény van, míg végtelen sok $R[x]$ -beli polinom, így vannak olyan polinomok, amikhez ugyanaz a polinomfüggvény tartozik, például $x, x^2 \in \mathbb{Z}_2[x]$.

Megjegyzés

Ha R végtelen elemszámú nullosztómentes gyűrű, akkor hiába van végtelen sok $R \rightarrow R$ függvény és végtelen sok $R[x]$ -beli polinom, mégis lesznek olyan függvények, amik nem tartozhatnak egyetlen polinomhoz sem annak polinomfüggvényeként.

Horner-elrendezés

Legyen $f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0$, ahol $f_n \neq 0$. Ekkor átrendezéssel a következő alakot kapjuk:

$$f(x) = (\dots((f_n \cdot x + f_{n-1}) \cdot x + f_{n-2}) \cdot x + \dots + f_1) \cdot x + f_0, \text{ és így}$$

$$f(c) = (\dots((f_n \cdot c + f_{n-1}) \cdot c + f_{n-2}) \cdot c + \dots + f_1) \cdot c + f_0.$$

Vagyis $f(c)$ kiszámítható n db szorzás és n db összeadás segítségével.

	f_n	f_{n-1}	f_{n-2}	\dots	f_0	
c	\times	$c_1 = f_n$	$c_2 = c_1 c + f_{n-1}$	\dots	$c_n = c_{n-1} c + f_1$	$f(c) = c_n c + f_0$

Általánosan: $c_k = c_{k-1} c + f_{n-k+1}$, ha $1 < k \leq n$.

Kicsit bőbeszédűbb (de kézzel írva követhetőbb) elrendezésben:

	f_n	f_{n-1}	f_{n-2}	\dots	f_1	f_0	
c	\times	$c \cdot c_1$	$c \cdot c_2$	\dots	$c \cdot c_{n-1}$	$c_n c$	
	$c_1 = f_n$	$c_2 = c_1 c + f_{n-1}$	$c_3 = c_2 c + f_{n-2}$	\dots	$c_n = c_{n-1} c + f_1$	$f(c) = c_n c + f_0$	

Horner-elrendezés

Példa

Határozzuk meg az $f(x) = x^4 - 3x^3 + x + 6$ polinom -2 helyen vett helyettesítési értékét!

	1	-3	0	1	6	
-2	×	1	-5	10	-19	44

Ha az $f(c)$ helyettesítési érték nulla, azaz, ha a c gyöke az f polinomnak, akkor a Horner-elrendezés alsó sorában (a helyettesítési érték előtt) annak a g polinomnak az együtthatói szerepelnek, amire $f(x) = (x - c) \cdot g(x)$.

Példa

Az $f(x) = x^4 - 4x^3 + 6x^2 - 4x + 1$ polinom $c = 1$ helyen vett helyettesítési értéke nulla:

	1	-4	6	-4	1	
1	×	1	-3	3	-1	0

Tehát $f(x) = (x - 1) \cdot (x^3 - 3x^2 + 3x - 1)$

A maradékos osztás tétele és következményei

Tétel (Polinomok maradékos osztása)

Legyen R egységelemes integritási tartomány, $f, g \in R[x]$, és tegyük fel, hogy g főegyütthatója egység R -ben. Ekkor egyértelműen léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = qg + r$, ahol $\deg(r) < \deg(g)$.

A fenti tétel az f polinomnak a g polinommal való maradékos elosztásának az egyértelmű elvégezhetőségét mondja ki.

A q polinomot a maradékos osztás **hányadospolinomjának**, az r polinomot az osztás **maradékpolinomjának** nevezzük.

A maradékos osztás tétele és következményei

Tétel (Polinomok maradékos osztása)

Legyen R egységelemes integritási tartomány, $f, g \in R[x]$, és tegyük fel, hogy g főegyütthatója egység R -ben. Ekkor egyértelműen léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = qg + r$, ahol $\deg(r) < \deg(g)$.

Bizonyítás

Létezés: f foka szerinti TI: Ha $\deg(f) < \deg(g)$, akkor $q = 0$ és $r = f$ esetén megfelelő előállítást kapunk.

Tfh. $\deg(f) \geq \deg(g)$. Legyen f főegyütthatója f_n , g főegyütthatója g_k . Mivel g_k egység, ezért $\exists g'_k \in R$, melyre $f_n = g'_k g_k$. Ekkor $g'_k x^{n-k} g(x)$ és $f(x)$ főtagja megegyezik, így $f^*(x) = f(x) - g'_k x^{n-k} g(x)$ -re $\deg(f^*) < \deg(f)$ (Miért?). Így f^* -ra használhatjuk az indukciós feltevést, vagyis léteznek $q^*, r^* \in R[x]$ polinomok, melyekre $f^* = q^* g + r^*$ és $\deg(r^*) < \deg(g)$. Ekkor

$$f(x) = f^*(x) + g'_k x^{n-k} g(x) = q^*(x)g(x) + r^*(x) + g'_k x^{n-k} g(x) = (q^*(x) + g'_k x^{n-k})g(x) + r^*(x),$$

így $q(x) = q^*(x) + g'_k x^{n-k} g(x)$ és $r(x) = r^*(x)$ jó választás.

A maradékos osztás tétele és következményei

Bizonyítás folyt.

Egyértelműség: Tekintsük f két megfelelő előállítását:

$f = qg + r = q^*g + r^*$, amiből:

$$g(q - q^*) = r^* - r.$$

A jobb oldali polinom foka:

$$\deg(r^* - r) \leq \max\{\deg(r^*), \deg(-r)\} = \deg(r^*) < \deg(g).$$

A bal oldali polinom foka: $\deg(g(q - q^*)) = \deg(g) + \deg(q - q^*)$, ami csak akkor kisebb mint $\deg(g)$, ha $\deg(q - q^*) < 0$, azaz, ha $q - q^*$ a nullpolinom, tehát, ha $q = q^*$, ahonnan $r = r^*$ is következik.

A maradékos osztás tétele és következményei

Definíció (gyöktényező)

Ha $c \in R$ az $f \in R[x]$ polinom gyöke, akkor $(x - c) \in R[x]$ a c -hez tartozó gyöktényező.

Következmény (Gyöktényező leválasztása)

Legyen R egységelemes integritási tartomány. Ha $f \in R[x]$, és $c \in R$ gyöke f -nek, akkor létezik olyan $q \in R[x]$, amelyre $f(x) = (x - c)q(x)$.

Bizonyítás

Osszuk el maradékosan f -et $(x - c)$ -vel (Miért lehet?):

$$f(x) = q(x)(x - c) + r(x).$$

Mivel $\deg(r(x)) < \deg(x - c) = 1$, ezért r konstans polinom.

Helyettesítsünk be c -t, így azt kapjuk, hogy

$$0 = f(c) = q(c)(c - c) + r(c) = r(c) = r, \text{ tehát } r = 0.$$

A maradékos osztás tétele és következményei

Következmény (Egységelemes integritási tartomány feletti polinom gyökeinek száma)

Az R egységelemes integritási tartomány fölötti $f \neq 0$ polinomnak legfeljebb $\deg(f)$ gyöke van.

Bizonyítás

f foka szerinti TI:

$\deg(f) = 0$ esetén igaz az állítás (Miért?).

Ha $\deg(f) > 0$, és $f(c) = 0$, akkor $f(x) = (x - c)g(x)$ (Miért?), ahol

$\deg(g) = \deg(f) - 1$ (Miért?). Ha d gyöke f -nek, akkor

$0 = f(d) = (d - c)g(d)$ azaz (Miért is?) vagy $d - c = 0$ (amiből $d = c$), vagy $g(d) = 0$, azaz d gyöke g -nek. Az indukciós feltevés szerint g -nek legfeljebb $\deg(g) = \deg(f) - 1$ gyöke van, ahonnan az állítás következik.

Ha R gyűrű **NEM** egységelemes integritási tartomány (például azért, mert vannak benne nullosztók), akkor nem igaz a fenti állítás.

Például \mathbb{Z}_6 fölött:

$$(x - 2)(x - 3) \equiv x^2 + x \equiv (x - 0)(x + 1) \pmod{6}$$

A maradékos osztás tétele és következményei

Következmény ($(n + 1)$ helyen megegyező legfeljebb n fokú polinomok)

Ha R egységelemes integritási tartomány, akkor ha két, legfeljebb n -ed fokú $R[x]$ -beli polinomnak $n + 1$ különböző helyen ugyanaz a helyettesítési értéke, akkor egyenlőek.

Bizonyítás

A két polinom különbsége legfeljebb n -ed fokú, és $n + 1$ gyöke van (Miért?), ezért nullpolinom (Miért?), vagyis a polinomok egyenlőek.

Következmény (Polinomok és polinomfüggvények kapcsolata végtelen egységelemes integritási tartomány felett)

Ha R végtelen egységelemes integritási tartomány, akkor két különböző $R[x]$ -beli polinomhoz nem tartozik ugyanaz a polinomfüggvény.

Bizonyítás

Ellenkező esetben a polinomok különbségének végtelen sok gyöke lenne (Miért?).

Bővített euklideszi algoritmus

Definíció (osztó és többszörös polinomgyűrűben)

Legyen R kommutatív gyűrű, $f, g \in R[x]$. Azt mondjuk, hogy g **osztója** f -nek (f **többszöröse** g -nek), ha létezik $h \in R[x]$, amire $f = g \cdot h$.

Definíció (polinomok legnagyobb közös osztója)

Legyen R kommutatív gyűrű. Az $f, g \in R[x]$ polinomok **legnagyobb közös osztójának** (**kitüntetett közös osztójának**) nevezünk egy olyan $d \in R[x]$ polinomot, amelyre $d|f$, $d|g$, és $\forall c \in R[x]$ esetén $(c|f \wedge c|g) \Rightarrow c|d$.

Testekben minden nem-nulla elem egység, így test fölötti polinomgyűrűben tetszőleges nem-nulla polinommal tudunk maradékosan osztani. Ezért működik az euklideszi és a bővített euklideszi algoritmus. Ha R test, akkor tetszőleges $f, g \in R[x]$ esetén a bővített euklideszi algoritmus meghatározza f és g (egy) legnagyobb közös osztóját: a $d \in R[x]$ polinomot, továbbá $u, v \in R[x]$ polinomokat, amelyekre $d = u \cdot f + v \cdot g$.

Bővített euklideszi algoritmus

Tétel (Bővített euklideszi algoritmus test feletti polinomgyűrűben)

Legyen R test, $f, g \in R[x]$. Ha $g = 0$, akkor az f és $g = 0$ polinomoknak f legnagyobb közös osztója és $f = 1 \cdot f + 0 \cdot g$. Ha $g \neq 0$, akkor végezzük el a következő maradékos osztásokat:

$$f = q_1 g + r_1;$$

$$g = q_2 r_1 + r_2;$$

$$r_1 = q_3 r_2 + r_3;$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n;$$

$$r_{n-1} = q_{n+1} r_n.$$

Ekkor $d = r_n$ az f és g egy legnagyobb közös osztója.

Az $u_{-1} = 1$, $u_0 = 0$, $v_{-1} = 0$, $v_0 = 1$ kezdőértékekkel, továbbá az $u_i = u_{i-2} - q_i \cdot u_{i-1}$ és $v_i = v_{i-2} - q_i \cdot v_{i-1}$ rekurziókkal megkapható $u = u_n$ és $v = v_n$ polinomokra teljesül $d = u \cdot f + v \cdot g$.

Bővített euklideszi algoritmus

Bizonyítás

A maradékok foka természetes számok szigorúan monoton csökkenő sorozata, ezért az eljárás véges sok lépésben véget ér.

Indukcióval belátjuk, hogy $r_{-1} = f$ és $r_0 = g$ jelöléssel $r_i = u_i \cdot f + v_i \cdot g$ teljesül minden $-1 \leq i \leq n$ esetén:

$i = -1$ -re $f = 1 \cdot f + 0 \cdot g$, $i = 0$ -ra $g = 0 \cdot f + 1 \cdot g$.

Mivel $r_i = r_{i-2} - q_i \cdot r_{i-1}$, így az indukciós feltevést használva:

$$\begin{aligned} r_i &= u_{i-2} \cdot f + v_{i-2} \cdot g - q_i \cdot (u_{i-1} \cdot f + v_{i-1} \cdot g) = \\ &= (u_{i-2} - q_i \cdot u_{i-1}) \cdot f + (v_{i-2} - q_i \cdot v_{i-1}) \cdot g = u_i \cdot f + v_i \cdot g. \end{aligned}$$

Tehát $r_n = u_n \cdot f + v_n \cdot g$, és így f és g közös osztói r_n -nek is osztói.

Kell még, hogy r_n osztója f -nek és g -nek.

Indukcióval belátjuk, hogy $r_n | r_{n-k}$ teljesül minden $0 \leq k \leq n+1$ esetén:

$k = 0$ -ra $r_n | r_n$ nyilvánvaló, $k = 1$ -re $r_{n-1} = q_{n+1} r_n$ miatt $r_n | r_{n-1}$.

$r_{n-(k+1)} = q_{n-(k-1)} r_{n-k} + r_{n-(k-1)}$ miatt az indukciós feltevést használva kapjuk az állítást, és így $k = n$, illetve $k = n+1$ helyettesítéssel $r_n | r_0 = g$, illetve $r_n | r_{-1} = f$.

Polinomok algebrai deriváltja

Definíció (polinomok algebrai deriváltja)

Legyen R gyűrű. Az

$f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_2 x^2 + f_1 x + f_0 \in R[x]$ ($f_n \neq 0$) polinom
algebrai deriváltja az

$f'(x) = n f_n x^{n-1} + (n-1) f_{n-1} x^{n-2} + \dots + 2 f_2 x + f_1 \in R[x]$ polinom.

Megjegyzés

Itt $k f_k = \underbrace{f_k + f_k + \dots + f_k}_{k \text{ db}}$. (Ez akkor kell, ha $k \in \mathbb{N}^+$, de $k \notin R$.)

Állítás

Legyen R gyűrű, $a, b \in R$ és $n \in \mathbb{N}^+$. Ekkor $(na)b = n(ab) = a(nb)$.

Bizonyítás

$$\underbrace{(a + a + \dots + a)}_{n \text{ db}} b = \underbrace{(ab + ab + \dots + ab)}_{n \text{ db}} = a \underbrace{(b + b + \dots + b)}_{n \text{ db}}$$

Polinomok algebrai deriváltja

Állítás (Az algebrai derivált tulajdonságai)

Ha R egységelemes integritási tartomány, akkor az $f \mapsto f'$ algebrai deriválás rendelkezik a következő tulajdonságokkal:

- 1 *konstans polinom deriváltja a nullpolinom;*
- 2 *az x polinom deriváltja az egységelem;*
- 3 *$(f + g)' = f' + g'$, ha $f, g \in R[x]$ (additivitás);*
- 4 *$(fg)' = f'g + fg'$, ha $f, g \in R[x]$ (szorzat differenciálási szabálya).*

Megjegyzés

Megfordítva, ha egy R egységelemes integritási tartomány esetén egy $f \mapsto f'$, $R[x]$ -et önmagába képező leképzés rendelkezik az előző 4 tulajdonsággal, akkor az az algebrai deriválás.

Polinomok algebrai deriváltja

Állítás $((x - c)^n)$ algebrai deriváltja

Ha R egységelemes integritási tartomány, $c \in R$ és $n \in \mathbb{N}^+$, akkor $((x - c)^n)' = n(x - c)^{n-1}$.

Bizonyítás

n szerinti TI:

$n = 1$ esetén $(x - c)' = 1 = 1 \cdot (x - c)^0$.

Tfh. $n = k$ -ra teljesül az állítás, vagyis $((x - c)^k)' = k(x - c)^{k-1}$.

Ekkor

$$\begin{aligned} ((x - c)^{k+1})' &= ((x - c)^k(x - c))' = ((x - c)^k)'(x - c) + (x - c)^k(x - c)' = \\ &= k(x - c)^{k-1}(x - c) + (x - c)^k \cdot 1 = (k + 1)(x - c)^k. \end{aligned}$$

Ezzel az állítást beláttuk.

Állítás (NB)

Ha R integritási tartomány, $\text{char}(R) = p$, és $0 \neq r \in R$, akkor $n \cdot r = 0 \iff p \mid n$.

Polinomok algebrai deriváltja

Definíció (polinom gyökének multiplicitása)

Legyen R egységelemes integritási tartomány, $0 \neq f \in R[x]$ és $n \in \mathbb{N}^+$. Azt mondjuk, hogy $c \in R$ az f egy n -szeres gyöke, ha $(x - c)^n | f$, de $(x - c)^{n+1} \nmid f$. Ekkor c multiplicitása n .

Megjegyzés

A definíció azzal ekvivalens, hogy $f(x) = (x - c)^n g(x)$, ahol c nem gyöke g -nek. (Miért?)

Tétel (Polinom gyökeinek multiplicitása és az algebrai derivált)

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $n \in \mathbb{N}^+$ és $c \in R$ az f egy n -szeres gyöke. Ekkor c az f' -nek legalább $(n - 1)$ -szeres gyöke, és ha $\text{char}(R) \nmid n$, akkor pontosan $(n - 1)$ -szeres gyöke.

Polinomok algebrai deriváltja

Bizonyítás

Ha $f(x) = (x - c)^n g(x)$, ahol c nem gyöke g -nek, akkor

$$\begin{aligned} f'(x) &= ((x - c)^n)' g(x) + (x - c)^n g'(x) = \\ &= n(x - c)^{n-1} g(x) + (x - c)^n g'(x) = (x - c)^{n-1} (ng(x) + (x - c)g'(x)). \end{aligned}$$

Tehát c tényleg legalább $(n - 1)$ -szeres gyöke f' -nek, és akkor lesz $(n - 1)$ -szeres gyöke, ha c nem gyöke $ng(x) + (x - c)g'(x)$ -nek, vagyis $0 \neq ng(c) + (c - c)g'(c) = ng(c) + 0 \cdot g'(c) = ng(c)$. Ez pedig teljesül, ha $\text{char}(R) \nmid n$.

Példa

Legyen $f(x) = x^4 - x \in \mathbb{Z}_3[x]$. Ekkor 1 3-szoros gyöke f -nek, mert

$$\begin{aligned} f(x) &= x(x^3 - 1) \stackrel{\mathbb{Z}_3}{=} x(x^3 - 3x^2 + 3x - 1) = x(x - 1)^3. \\ f'(x) &= (x - 1)^3 + 3x(x - 1)^2 = (x - 1)^2(4x - 1) \stackrel{\mathbb{Z}_3}{=} \\ &\stackrel{\mathbb{Z}_3}{=} (x - 1)^2(x - 1) = (x - 1)^3, \end{aligned}$$

tehát 1 3-szoros gyöke f' -nek is.

Lagrange-interpoláció

Tétel (Lagrange-interpoláció)

Legyen R test, $c_0, c_1, \dots, c_n \in R$ különbözőek, továbbá $d_0, d_1, \dots, d_n \in R$ tetszőlegesek. Ekkor létezik egy olyan legfeljebb n -ed fokú polinom, amelyre $f(c_j) = d_j$, ha $j = 0, 1, \dots, n$.

Bizonyítás

Legyen

$$\ell_j(x) = \frac{\prod_{i \neq j} (x - c_i)}{\prod_{i \neq j} (c_j - c_i)},$$

a j -edik Lagrange-interpolációs alappolinom, és legyen

$$f(x) = \sum_{j=0}^n d_j \ell_j(x).$$

$\ell_j(c_i) = 0$, ha $i \neq j$, és $\ell_j(c_j) = 1$ -ből következik az állítás.

Lagrange-interpoláció

Példa

Adjunk meg olyan $f \in \mathbb{R}[x]$ polinomot, amelyre $f(0) = 3$, $f(1) = 3$, $f(4) = 7$ és $f(-1) = 0$!

A feladat szövege alapján $c_0 = 0$, $c_1 = 1$, $c_2 = 4$, $c_3 = -1$, $d_0 = 3$, $d_1 = 3$, $d_2 = 7$ és $d_3 = 0$ értékekkel alkalmazzuk a Lagrange-interpolációt.

$$\ell_0(x) = \frac{(x-1)(x-4)(x+1)}{(0-1)(0-4)(0+1)} = \frac{1}{4}x^3 - x^2 - \frac{1}{4}x + 1$$

$$\ell_1(x) = \frac{(x-0)(x-4)(x+1)}{(1-0)(1-4)(1+1)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 + \frac{2}{3}x$$

$$\ell_2(x) = \frac{(x-0)(x-1)(x+1)}{(4-0)(4-1)(4+1)} = \frac{1}{60}x^3 - \frac{1}{60}x$$

$$\ell_3(x) = \frac{(x-0)(x-1)(x-4)}{(-1-0)(-1-1)(-1-4)} = -\frac{1}{10}x^3 + \frac{1}{2}x^2 - \frac{2}{5}x$$

$$f(x) = 3\ell_0(x) + 3\ell_1(x) + 7\ell_2(x) + 0\ell_3(x) = \frac{22}{60}x^3 - \frac{3}{2}x^2 + \frac{68}{60}x + 3$$

	$\frac{22}{60}$	$-\frac{3}{2}$	$\frac{68}{60}$	3	
1	X	$\frac{22}{60}$	$-\frac{68}{60}$	0	3
4	X	$\frac{22}{60}$	$-\frac{2}{60}$	1	7
-1	X	$\frac{22}{60}$	$-\frac{112}{60}$	3	0

Lagrange-interpoláció

Alkalmazás

A Lagrange-interpoláció használható titokmegosztásra a következő módon:

legyenek $1 \leq m < n$ egészek, továbbá $s \in \mathbb{N}$ a titok, amit n ember között akarunk szétosztani úgy, hogy bármely m részből a titok rekonstruálható legyen, de kevesebből nem. Válasszunk a titok maximális lehetséges értékénél és n -nél is nagyobb p prímet, továbbá $a_1, a_2, \dots, a_{m-1} \in \mathbb{Z}_p$ véletlen együtthatókat, majd határozzuk meg az

$f(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \dots + a_1x + s$ polinomra az $f(i)$ értékeket, és adjuk ezt meg az i . embernek ($i = 1, 2, \dots, n$).

Bármely m helyettesítési értékből a Lagrange-interpolációval megkapható a polinom, így annak konstans tagja is, a titok.

Ha m -nél kevesebb helyettesítési értékünk van, akkor nem tudjuk meghatározni a titkot, mert tetszőleges t esetén az $f(0) = t$ értéket hozzávéve a többihez létezik olyan legfeljebb m -ed fokú polinom, aminek a konstans tagja t , és az adott helyeken megfelelő a helyettesítési értéke.

Titokmegosztás

Példa

Legyen $m = 3$, $n = 4$, $s = 5$, $p = 7$, továbbá $a_1 = 3$ és $a_2 = 4$. Ekkor $f(x) = 4x^2 + 3x + 5 \in \mathbb{Z}_7[x]$, a titokrészletek pedig $f(1) = 5$, $f(2) = 6$, $f(3) = 1$ és $f(4) = 4$. Ha rendelkezünk például az $f(1) = 5$, $f(3) = 1$ és $f(4) = 4$ információkkal, akkor $c_0 = 1$, $c_1 = 3$, $c_2 = 4$, $d_0 = 5$, $d_1 = 1$, és $d_2 = 4$ értékekkel alkalmazzuk a Lagrange-interpolációt.

$$\ell_0(x) = \frac{(x-3)(x-4)}{(1-3)(1-4)} = \frac{1}{6}(x^2 - 7x + 12) = \frac{1}{-1}(-6x^2 - 2) = 6x^2 + 2$$

$$\ell_1(x) = \frac{(x-1)(x-4)}{(3-1)(3-4)} = -\frac{1}{2}(x^2 - 5x + 4) = -4(x^2 + 2x + 4) = 3x^2 + 6x + 5$$

$$\ell_2(x) = \frac{(x-1)(x-3)}{(4-1)(4-3)} = \frac{1}{3}(x^2 - 4x + 3) = 5(x^2 + 3x + 3) = 5x^2 + x + 1$$

$$\begin{aligned} f(x) &= 5\ell_0(x) + \ell_1(x) + 4\ell_2(x) = 30x^2 + 10 + 3x^2 + 6x + 5 + 20x^2 + 4x + 4 = \\ &= 53x^2 + 10x + 19 = 4x^2 + 3x + 5 \end{aligned}$$

Polinomok felbonthatósága

Definíció (felbonthatatlan és felbontható polinomok)

Legyen R egységelemes integritási tartomány. Egy $0 \neq f \in R[x]$ nem egység polinomot pontosan akkor nevezünk **felbonthatatlannak** (**irreducibilisnek**), ha $\forall a, b \in R[x]$ -re

$$f = a \cdot b \implies (a \text{ egység} \vee b \text{ egység}).$$

Ha a $0 \neq f \in R[x]$ polinom nem egység és nem felbonthatatlan, akkor **felbonthatónak** (**reducibilisnek**) nevezzük.

Megjegyzés

Utóbbi azt jelenti, hogy f -nek van nemtriviális szorzat-előállítás (olyan, amiben egyik tényező sem egység).

A konstans nulla polinom és az egység polinomok se nem felbonthatatlanok, se nem felbonthatók.

Polinomok felbonthatósága

Állítás (Egységek test feletti polinomgyűrűben)

Legyen $(F; +, \cdot)$ test. Ekkor $f \in F[x]$ pontosan akkor egység, ha $\deg(f) = 0$.

Bizonyítás

\Leftarrow

Ha $\deg(f) = 0$, akkor f nem-nulla konstans polinom: $f(x) = f_0$. Mivel F test, ezért létezik $f_0^{-1} \in F$, amire $f_0 \cdot f_0^{-1} = 1$, ezért minden $g(x) \in F[x]$ -re $g = f_0 \cdot f_0^{-1} \cdot g = f \cdot (f_0^{-1} \cdot g)$, tehát f osztja g -t, így f tényleg egység.

\Rightarrow

Ha f egység, akkor létezik $g \in F[x]$, amire $f \cdot g = 1$, és így $\deg(f) + \deg(g) = \deg(1) = 0$ (Miért?), ami csak $\deg(f) = \deg(g) = 0$ esetén lehetséges.

Polinomok felbonthatósága

Állítás (Test feletti elsőfokú polinomok)

Legyen $(F; +, \cdot)$ test, és $f \in F[x]$. Ha $\deg(f) = 1$, akkor f -nek van gyöke.

Bizonyítás

Ha $\deg(f) = 1$, akkor felírható $f(x) = f_1x + f_0$ alakban, ahol $f_1 \neq 0$. Azt szeretnénk, hogy létezzen $c \in F$, amire $f(c) = 0$, vagyis $f_1c + f_0 = 0$. Ekkor $f_1c = -f_0$ (Miért?), és mivel létezik $f_1^{-1} \in F$, amire $f_1 \cdot f_1^{-1} = 1$ (Miért?), ezért $c = -f_0 \cdot f_1^{-1} \left(= -\frac{f_0}{f_1} \right)$ gyök lesz.

Megjegyzés

Ha $(R; +, \cdot)$ nem test, akkor egy R fölötti elsőfokú polinomnak nem feltétlenül van gyöke, pl. $2x - 1 \in \mathbb{Z}[x]$ polinomnak nincs egész gyöke. (És emlékezzünk, hogy $R[x]$ -beli polinomnak csak R -beli gyökeit definiáltuk. . .)

Polinomok felbonthatósága

Állítás (Test feletti elsőfokú polinomok felbonthatatlansága)

Legyen $(F; +, \cdot)$ test, és $f \in F[x]$. Ha $\deg(f) = 1$, akkor f felbonthatatlan.

Bizonyítás

Legyen $f = g \cdot h$. Ekkor $\deg(g) + \deg(h) = \deg(f) = 1$ (Miért?) miatt $\deg(g) = 0 \wedge \deg(h) = 1$ vagy $\deg(g) = 1 \wedge \deg(h) = 0$. Előbbi esetben g , utóbbiban h egység a korábbi állítás értelmében.

Megjegyzés

Tehát nem igaz, hogy egy felbonthatatlan polinomnak nem lehet gyöke.

Polinomok felbonthatósága

Állítás (Test feletti másod- és harmadfokú polinomok felbonthatósága)

Legyen $(F; +, \cdot)$ test, és $f \in F[x]$. Ha $2 \leq \deg(f) \leq 3$, akkor f pontosan akkor felbontható, ha van gyöke.

Bizonyítás

←

Ha c gyöke f -nek, akkor az $f(x) = (x - c)g(x)$ egy nemtriviális felbontás (Miért?).

⇒

Mivel $2 = 0 + 2 = 1 + 1$, illetve $3 = 0 + 3 = 1 + 2$, és más összegként nem állnak elő, ezért amennyiben f -nek van nemtriviális felbontása, akkor van elsőfokú osztója. A korábbi állítás alapján ennek van gyöke, és ez nyilván f gyöke is lesz.

Polinomok felbonthatósága \mathbb{C} felett

Tétel (Felbonthatatlan polinomok \mathbb{C} felett)

$f \in \mathbb{C}[x]$ pontosan akkor felbonthatatlan, ha $\deg(f) = 1$.

Bizonyítás

←

Mivel \mathbb{C} a szokásos műveletekkel test, ezért korábbi állítás alapján teljesül.

⇒

Indirekt tfh. $\deg(f) \neq 1$. Ha $\deg(f) < 1$, akkor $f = 0$ vagy f egység, tehát nem felbonthatatlan, ellentmondásra jutottunk.

$\deg(f) > 1$ esetén az algebra alaptétele értelmében van gyöke f -nek. A gyöktényezőt kiemelve az $f(x) = (x - c)g(x)$ alakot kapjuk, ahol $\deg(g) \geq 1$ (Miért?), vagyis egy nemtriviális szorzat-előállítást, így f nem felbonthatatlan, ellentmondásra jutottunk.

Az algebra alaptételét itt használtuk, de nem bizonyítottuk!

Polinomok felbonthatósága \mathbb{R} felett

Tétel (Felbonthatatlan polinomok \mathbb{R} felett)

$f \in \mathbb{R}[x]$ pontosan akkor felbonthatatlan, ha

- $\deg(f) = 1$, vagy
- $\deg(f) = 2$, és f -nek nincs (valós) gyöke.

Bizonyítás



Ha $\deg(f) = 1$, akkor korábbi állítás (test fölötti elsőfokú polinom...) alapján f felbonthatatlan.

Ha $\deg(f) = 2$, és f -nek nincs gyöke, akkor korábbi állítás (test fölötti másodfokú polinom...) alapján f felbonthatatlan.



Ha f felbonthatatlan, akkor nem lehet $\deg(f) < 1$. (Miért?)

Ha f felbonthatatlan, és $\deg(f) = 2$, akkor nem lehet gyöke. (Miért?)

De még nem vagyunk kész! Még nem láttuk, hogy ne lehetne kettőnél magasabb fokú egy \mathbb{R} felett irreducibilis polinom...

Polinomok felbonthatósága \mathbb{R} felett

Bizonyítás folyt.

Tfh. $\deg(f) \geq 3$. Az algebra alaptétele értelmében f -nek mint \mathbb{C} fölötti polinomnak van $c \in \mathbb{C}$ gyöke. Ha $c \in \mathbb{R}$ is teljesül, akkor a gyöktényező kiemelésével f egy nemtriviális felbontását kapjuk (Miért?), ami ellentmondás.

Legyen most $c \in \mathbb{C} \setminus \mathbb{R}$ gyöke f -nek, és tekintsük a

$g(x) = (x - c)(x - \bar{c}) = x^2 - 2\operatorname{Re}(c)x + |c|^2 \in \mathbb{R}[x]$ polinomot.

f -et g -vel maradékosan osztva létezik $q, r \in \mathbb{R}[x]$, hogy $f = qg + r$.

$r = 0$, mert $\deg(r) < 2$, és r -nek gyöke $c \in \mathbb{C} \setminus \mathbb{R}$.

Vagyis $f = qg$, ami egy nemtriviális felbontás, ez pedig ellentmondás.

Megjegyzés

Ha $f \in \mathbb{R}[x]$ -nek $c \in \mathbb{C}$ gyöke, akkor \bar{c} is gyöke, hiszen

$$f(\bar{c}) = \sum_{j=0}^{\deg(f)} f_j(\bar{c})^j = \sum_{j=0}^{\deg(f)} \bar{f}_j \cdot \bar{c}^j = \sum_{j=0}^{\deg(f)} \bar{f}_j \bar{c}^j = \overline{\left(\sum_{j=0}^{\deg(f)} f_j c^j \right)} = \overline{f(c)} = \bar{0} = 0.$$

Polinomok felbonthatósága \mathbb{Z} felett

Definíció (primitív polinom)

$f \in \mathbb{Z}[x]$ -et **primitív polinomnak** nevezzük, ha az együtthatóinak a legnagyobb közös osztója 1 .

Lemma (Gauss)

Ha $f, g \in \mathbb{Z}[x]$ primitív polinomok, akkor fg is primitív polinom.

Bizonyítás

Indirekt tfh. fg nem primitív polinom. Ekkor van olyan $p \in \mathbb{Z}$ prím, ami osztja fg minden együtthatóját. Legyen i , illetve j a legkisebb olyan index, amire $p \nmid f_i$, illetve $p \nmid g_j$ (Miért vannak ilyenek?). Ekkor fg -nek az $(i+j)$ indexű együtthatója $f_0g_{i+j} + \dots + f_i g_j + \dots + f_{i+j}g_0$, és ebben az összegben p nem osztója $f_i g_j$ -nek, de osztója az összes többi tagnak (Miért?), de akkor nem osztója az összegnek, ami ellentmondás.

Polinomok felbonthatósága \mathbb{Z} felett

Állítás (\mathbb{Z} feletti polinom felírása primitív polinom segítségével)

Minden $0 \neq f \in \mathbb{Z}[x]$ polinom felírható $f = df^*$ alakban, ahol $0 \neq d \in \mathbb{Z}$, és $f^* \in \mathbb{Z}[x]$ egy primitív polinom.

Bizonyítás

Ha f -ből az együtthatók legnagyobb közös osztóját kiemeljük, és azt d -nek választjuk, akkor megkapjuk a megfelelő előállítást.

Megjegyzés

Az előállítás lényegében (előjelektől eltekintve) egyértelmű, így f^* főegyütthatóját pozitívnak választva egyértelmű.

Polinomok felbonthatósága \mathbb{Z} felett

Állítás (\mathbb{Q} feletti polinom feírása primitív polinom segítségével)

Minden $0 \neq f \in \mathbb{Q}[x]$ polinom felírható $f = af^*$ alakban, ahol $0 \neq a \in \mathbb{Q}$, és $f^* \in \mathbb{Z}[x]$ egy primitív polinom.

Bizonyítás

Írjuk fel f együtthatóit egész számok hányadosaiként. Ha végigszorozzuk f -et az együtthatói nevezőinek c szorzatával, majd kiemeljük a kapott $\mathbb{Z}[x]$ -beli polinom együtthatóinak d legnagyobb közös osztóját, akkor megkapjuk a megfelelő előállítást $a = d/c$ -vel.

Megjegyzés

Az előállítás lényegében egyértelmű: ha f^* főegyütthatóját pozitívnak választjuk, akkor egyértelmű.

Polinomok felbonthatósága $\mathbb{Z}[x]$ felett

Tétel (Gauss tétele $\mathbb{Z}[x]$ -re)

Ha egy $f \in \mathbb{Z}[x]$ előállítható két nem konstans $g, h \in \mathbb{Q}[x]$ polinom szorzataként, akkor előállítható két nem konstans $g^*, h^* \in \mathbb{Z}[x]$ polinom szorzataként is.

Bizonyítás

Tfh. $f = gh$, ahol $g, h \in \mathbb{Q}[x]$ nem konstans polinomok. Legyen $f = df^*$, ahol $d \in \mathbb{Z}$, és $f^* \in \mathbb{Z}[x]$ primitív polinom, aminek a főegyütthatója pozitív. Ha felírjuk g -t ag^{**} , h -t pedig bh^{**} alakban, ahol $g^{**}, h^{**} \in \mathbb{Z}[x]$ primitív polinomok, amiknek a főegyütthatója pozitív, akkor azt kapjuk, hogy $df^* = f = gh = abg^{**} \cdot h^{**}$. Mivel Gauss lemmája szerint $g^{**} \cdot h^{**}$ is primitív polinom, továbbá f előállítására primitív polinom segítségével lényegében egyértelmű, ezért $f^* = g^{**} h^{**}$, és $d = ab$, vagyis $f = dg^{**} h^{**}$, és például $g^* = dg^{**}$, $h^* = h^{**}$ választással kapjuk f kívánt felbontását.

Polinomok felbonthatósága \mathbb{Z} felett

Következmény

$f \in \mathbb{Z}[x]$ primitív polinom pontosan akkor felbontható \mathbb{Z} fölött, amikor felbontható \mathbb{Q} fölött.

Bizonyítás

\Rightarrow

A \mathbb{Z} fölötti felbontás egyben \mathbb{Q} fölötti felbontás is.

\Leftarrow

A Gauss-tételből következik az állítás.

Polinomok felbonthatósága \mathbb{Z} felett

Tétel (Schönemann-Eisenstein-kritérium)

Legyen $f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ legalább elsőfokú primitív polinom. Ha található olyan $p \in \mathbb{Z}$ prím, melyre

- $p \nmid f_n$,
- $p \mid f_j$, ha $0 \leq j < n$,
- $p^2 \nmid f_0$,

akkor f felbonthatatlan \mathbb{Z} fölött.

Bizonyítás

Tfh. $f = gh$. Mivel p nem osztja f főegyütthatóját, ezért sem a g , sem a h főegyütthatóját nem osztja (Miért?). Legyen m a legkisebb olyan index, amelyre $p \nmid g_m$, és o a legkisebb olyan index, amelyre $p \nmid h_o$. Ha $k = m + o$, akkor

$$p \nmid f_k = \sum_{i+j=k} g_i h_j,$$

mivel p osztja az összeg minden tagját, kivéve azt, amelyben $i = m$ és $j = o$.

Polinomok felbonthatósága \mathbb{Z} felett

Megjegyzések

- A feltételben f_n és f_0 szerepe felcserélhető.
- A tétel nem használható test fölötti polinom irreducibilitásának bizonyítására, mert testben nem léteznek prímek, hiszen minden nem-nulla elem egység.

Racionális gyökteszt

Tétel (Racionális gyökteszt)

Legyen $f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ primitív polinom. Ha $f\left(\frac{p}{q}\right) = 0$, $p, q \in \mathbb{Z}$, $(p, q) = 1$, akkor $p \mid f_0$ és $q \mid f_n$.

Bizonyítás

$$0 = f\left(\frac{p}{q}\right) = f_n \left(\frac{p}{q}\right)^n + f_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + f_1 \left(\frac{p}{q}\right) + f_0 \quad / \cdot q^n$$

$$0 = f_n p^n + f_{n-1} q p^{n-1} + \dots + f_1 q^{n-1} p + f_0 q^n$$

$p \mid f_0 q^n$, mivel az összes többi tagnak osztója p , és így $(p, q) = 1$ miatt $p \mid f_0$.

$q \mid f_n p^n$, mivel az összes többi tagnak osztója q , és így $(p, q) = 1$ miatt $q \mid f_n$.

Megjegyzés

f primitívsege nem szükséges feltétel, csak praktikus. (Miért?)

A racionális gyökteszt alkalmazása

Állítás ($\sqrt{2}$ irracionális)

$$\sqrt{2} \notin \mathbb{Q}.$$

Bizonyítás

Tekintsük az $x^2 - 2 \in \mathbb{Z}[x]$ polinomot.

Ennek a $\frac{p}{q}$ alakú gyökeire ($p, q \in \mathbb{Z}, (p, q) = 1$) teljesül, hogy $p|2$ és $q|1$, így a lehetséges racionális gyökei ± 1 és ± 2 .

Véges testek

Tekintsük valamely p prímre a \mathbb{Z}_p testet, továbbá egy $f(x) \in \mathbb{Z}_p[x]$ felbonthatatlan főpolinomot. Vezessük be a $g(x) \equiv h(x) \pmod{f(x)}$, ha $f(x) | g(x) - h(x)$ relációt.

Ez ekvivalenciareláció, ezért meghatároz egy osztályozást $\mathbb{Z}_p[x]$ -en.

Minden osztálynak van $\deg(f)$ -nél alacsonyabb fokú reprezentánsa (Miért?), és ha $\deg(g), \deg(h) < \deg(f)$, továbbá g és h ugyanabban az osztályban van, akkor egyenlőek (Miért?). Tehát $\deg(f) = n$ esetén bijekciót létesíthetünk az n -nél kisebb fokú polinomok és az osztályok között, így p^n darab osztály van.

Az osztályok között értelmezhetjük a természetes módon a műveleteket. Ezeket végezhetjük az n -nél alacsonyabb fokú reprezentánsokkal: ha a szorzat foka nem kisebb, mint n , akkor az $f(x)$ -szel vett osztási maradékot vesszük.

Véges testek

$f \nmid g$ esetén a bővített euklideszi algoritmus alapján

$$d(x) = u(x)f(x) + v(x)g(x).$$

Mivel $f(x)$ felbonthatatlan, ezért $d(x) = d$ konstans polinom, így $\frac{v(x)}{d}$ multiplikatív inverze lesz $g(x)$ -nek.

Tétel (NB)

Az ekvivalenciaosztályok halmaza a rajta értelmezett összeadással és szorzással testet alkot.

Megjegyzés

Tetszőleges p prím és n pozitív egész esetén létezik p^n elemű test, mert létezik n -ed fokú felbonthatatlan polinom \mathbb{Z}_p -ben.

Megjegyzés

Véges test elemszáma prímszám, továbbá az azonos elemszámú testek izomorfak.

Véges testek

Példa

Tekintsük az $x^2 + 1 \in \mathbb{Z}_3[x]$ felbonthatatlan polinomot (Miért az?). A legfeljebb elsőfokú polinomok: $0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$. Az összeadás műveleti táblája:

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1

Például:

$$2x + 2 + 2x + 1 = 4x + 3 \stackrel{\mathbb{Z}_3}{=} x$$

Véges testek

Példa folyt.

·	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x	2x+2	x	1
2x+2	0	2x+2	x+1	2x+1	x	2	x+2	1	2x

Például:

$$(2x + 2)(2x + 1) = 4x^2 + 6x + 2 \stackrel{\mathbb{Z}_3}{=} x^2 + 2 = (x^2 + 1) + 1$$

Feladat: Legyen $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 1)$. Mik lesznek a $z^2 + 1 \in \mathbb{F}_9[z]$ polinom gyökei?