1. A maradékos osztás

Egész számok osztása.

Példa

$$
\begin{array}{rl}
223 : 7 = & \boxed{31} \\
-21 & \\
\hline
13 & \\
-7 & \\
\hline
\boxed{6} &
\end{array}
$$

$223 = 7 \cdot 31 + 6.$

Visszaszorzunk
Kivonunk

Állítás (számelméletből)
Minden $a, b \in \mathbb{Z}$ esetén, ahol $b \neq 0$, létezik olyan $q, r \in \mathbb{Z}$, hogy $a = bq + r$ és $|r| < |b|$.

Polinomok osztása.

Példa

$$
\begin{array}{l}
(2x^3 + \ 2x^2 + 3x \ + 2) \ : \ (x^2 + 1) = \boxed{2x + 2} \\
-\ (2x^3 + \quad 0 \ \ + 2x) \\
\hline
\qquad 2x^2 + \ x \ \ + 2 \\
\quad -\ (2x^2 + \ 0 \ \ + 2) \\
\hline
\qquad\qquad \boxed{x}
\end{array}
$$

$2x^3 + 2x^2 + 3x + 2 = (x^2 + 1)(2x + 2) + x.$

$(2x^3)/x^2 = 2x$
Visszaszorzunk: $(2x)(x^2 + 1) = 2x^3 + 2x$
Kivonunk
$(2x^2)/x^2 = 2$
Visszaszorzunk: $2(x^2 + 1) = 2x^2 + 2$
Kivonunk

Tétel
Minden $f, g \in \mathbb{C}[x]$ esetén, ahol $g \neq 0$, létezik olyan $q, r \in \mathbb{C}[x]$, hogy $f = gq + r$, és $r = 0$, vagy $\mathrm{gr}(r) < \mathrm{gr}(g)$. A q és r egyértelműen meghatározott.

Maradékos osztás: létezés.

Tétel
Minden $f, g \in \mathbb{C}[x]$ esetén, ahol $g \neq 0$, *létezik* olyan $q, r \in \mathbb{C}[x]$, hogy $f = gq + r$, és $r = 0$, vagy $\mathrm{gr}(r) < \mathrm{gr}(g)$.

Bizonyítás
$\mathrm{gr}(f)$ szerinti indukció. Ha $f = 0$, vagy $\mathrm{gr}(f) < \mathrm{gr}(g)$: $f = g \cdot 0 + f$. Tegyük föl: $\mathrm{gr}(f) = n \geq \mathrm{gr}(g)$, és az n-nél kisebb fokúakra igaz. Legyen f főtagja ax^n és g főtagja bx^m, ahol $b \neq 0$ és $m \leq n$. Ekkor $f_0 = f - (a/b)x^{n-m}g$-ből kiesik az n-edfokú tag. Indukciós feltevés: $f_0 = gq_0 + r$, ahol $r = 0$, vagy $\mathrm{gr}(r) < \mathrm{gr}(g)$. $f = f_0 + (a/b)x^{n-m}g = g\big(q_0 + (a/b)x^{n-m}\big) + r$. Tehát f is elosztható maradékosan g-vel. □

A q és r együtthatói a négy alapművelettel kaphatók. Az eljárás során csak g főegyütthatójával osztunk.

Maradékos osztás: együtthatók.

Tétel
Minden $f, g \in \mathbb{C}[x]$ esetén, ahol $g \neq 0$, *létezik* olyan $q, r \in \mathbb{C}[x]$, hogy $f = gq + r$, és $r = 0$, vagy $\mathrm{gr}(r) < \mathrm{gr}(g)$.

A q és r együtthatói a négy alapművelettel kaphatók. Az eljárás során csak g főegyütthatójával osztunk.

Következmény
Lehet maradékosan osztani $\mathbb{R}[x]$-ben és $\mathbb{Q}[x]$-ben is. Oka: $\mathbb{R}$-ben és $\mathbb{Q}$-ban minden nem nulla számmal oszthatunk.

Következmény
$\mathbb{Z}[x]$-ben oszthatunk maradékosan az olyan polinomokkal, *amelyek főegyütthatója* 1 *vagy* -1. Oka: $\mathbb{Z}$-ben 1-gyel és -1-gyel minden számot eloszthatunk.

Maradékos osztás *NINCS* $\mathbb{Z}[x]$-ben.

Példa
A $x : 2$ maradékos osztás nem végezhető el $\mathbb{Z}[x]$-ben.

Bizonyítás
Indirekt föltevés: $x = 2q + r$, ahol $q, r \in \mathbb{Z}[x]$, és $r = 0$ vagy $\mathrm{gr}(r) < \mathrm{gr}(2)$. De $\mathrm{gr}(r) < \mathrm{gr}(2) = 0$ nem lehet, tehát $r = 0$, azaz $x = 2q(x)$. Ez lehetetlen, például $x = 1$-et helyettesítve azt kapjuk, hogy $1 = 2q(1)$, azaz 1 páros szám, ami ellentmondás. □

Megjegyzés
$\mathbb{Q}[x]$-ben $x : 2$-nél a hányados $x/2$, a maradék 0. Így a maradékos osztás egyértelműségéből is látszik, hogy $x : 2$ nem végezhető el $\mathbb{Z}[x]$-ben, hiszen $x/2 \notin \mathbb{Z}[x]$.

Maradékos osztás: egyértelműség.

Tétel
Legyen $f, g \in \mathbb{C}[x]$, ahol $g \neq 0$. $f = gq_1 + r_1$, ahol $r_1 = 0$, vagy $\mathrm{gr}(r_1) < \mathrm{gr}(g)$. $f = gq_2 + r_2$, ahol $r_2 = 0$, vagy $\mathrm{gr}(r_2) < \mathrm{gr}(g)$. Ekkor $q_1 = q_2$ és $r_1 = r_2$.

Bizonyítás
$gq_1+r_1 = f = gq_2+r_2$, átrendezéssel $g(q_1-q_2) = r_2-r_1$. Itt r_2-r_1 vagy nulla, vagy g-nél kisebb fokú. Ha $q_1-q_2 \neq 0$, akkor $\mathrm{gr}\big(g(q_1-q_2)\big) = \mathrm{gr}(g)+\mathrm{gr}(q_1-q_2) \geq \mathrm{gr}(g)$. Ez ellentmondás, tehát $q_1 - q_2 = 0$, és így $q_1 = q_2$. De akkor $r_2 - r_1 = g \cdot 0 = 0$, és így $r_1 = r_2$. □

Lásd Kiss-jegyzet, 3.2. Szakasz.

2. Oszthatóság polinomok között

Oszthatóság.

Definíció
Legyen R a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ egyike.
Azt mondjuk, hogy a $g \in R[x]$ polinom *osztója* $f \in R[x]$-nek $R[x]$-ben, ha létezik olyan $h \in R[x]$ polinom, hogy $f(x) = g(x)h(x)$. Jelölés: $g \mid f$ (vagy néha $g \mid_{R[x]} f$).

Példák
$x + 1$ osztója $x^2 - 1$-nek $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ mindegyikében,
mert $x^2 - 1 = (x + 1)(x - 1)$, és $x + 1 \in \mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.

2 osztója x-nek $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ mindegyikében,
mert $x = 2(x/2)$, és $x/2 \in \mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$.

2 *nem* osztója x-nek $\mathbb{Z}[x]$-ben, mert ha $2h(x) = x$ lenne,
ahol $h(x) = c_0 + c_1x + \ldots$, és $c_0, c_1, \ldots$ egészek, akkor x együtthatóját véve $2c_1 = 1$ teljesülne.

A hányados együtthatói.

Következmény (Kiss-jegyzet, 3.2.2. Állítás)
Tegyük föl, hogy $g(x)$ osztója $f(x)$-nek $\mathbb{C}[x]$-ben, és $f, g \in \mathbb{R}[x]$. Ekkor $g \mid f$ teljesül $\mathbb{R}[x]$-ben is.

Bizonyítás
A feltevés szerint $f(x) = g(x)h(x)$, ahol $h \in \mathbb{C}[x]$. Osszuk el maradékosan f-et g-vel $\mathbb{R}[x]$-ben:

$$f = gq + r,$$

ahol $q, r \in \mathbb{R}[x]$ és $r = 0$, vagy $\mathrm{gr}(r) < \mathrm{gr}(g)$. Ez $\mathbb{C}[x]$-ben is egy maradékos osztás. De $\mathbb{C}[x]$-ben

$$f = gh + 0$$

is egy maradékos osztás. A $\mathbb{C}[x]$-beli *egyértelműség* miatt $q(x) = h(x)$. De $q \in \mathbb{R}[x]$, ezért $h \in \mathbb{R}[x]$. □

Ugyanígy $\mathbb{R}$ helyett $\mathbb{Q}$-ra is.

Egységek.

Definíció
Legyen R a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ egyike.
Azt mondjuk, hogy a $g \in R[x]$ polinom *egység* $R[x]$-ben, ha minden $R[x]$-beli polinomnak osztója $R[x]$-ben.

Tétel (Kiss-jegyzet, 3.1.11. Gyakorlat)
$\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ egységei a nem nulla konstans polinomok.
$\mathbb{Z}[x]$ egységei csak az 1 és a -1.

Bizonyítás (vázlat)
Ha $g(x)$ egység, akkor osztója a konstans 1 polinomnak, azaz van reciproka. Láttuk (fokszámmal), hogy g konstans. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$-ban minden nem nulla számmal lehet osztani, $\mathbb{Z}$-ben csak ± 1-gyel osztható minden szám.

Kitüntetett közös osztó.

Definíció
Legyen R a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ egyike.
Azt mondjuk, hogy $h(x)$ az $f, g \in R[x]$ polinomok *kitüntetett közös osztója* $R[x]$-ben, ha *közös osztójuk*, azaz $h \mid f$ és $h \mid g$, továbbá *h az f és g minden közös osztójának többszöröse*, azaz tetszőleges k polinomra $k \mid f$ és $k \mid g$ esetén $k \mid h$.

Mint számelméletben (Kiss-jegyzet, 3.1 és 3.2. Szakasz)
A kitüntetett közös osztó egységszeres erejéig *egyértelműen meghatározott*. Azaz ha h_1 és h_2 is kitüntetett közös osztója f-nek és g-nek, akkor h_1 és h_2 egymás egységszeresei.

Az f és g kitüntetett közös osztója $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött az *euklideszi algoritmussal* számítható ki, és fölírható $f(x)u(x) + g(x)v(x)$ alakban alkalmas $u(x)$, $v(x)$-re.

3. Konjugált gyökök

Az algebra alaptételének következménye.

Beláttuk
Minden n-edfokú komplex együtthatós f polinom fölírható $c(x-b_1)\dots(x-b_n)$ alakban, ahol c az f főegyütthatója. Ez az f polinom *gyöktényezős alakja*.

Beláttuk
Minden n-edfokú komplex együtthatós polinomnak multiplicitásokkal számolva n darab gyöke van.

Állítás
Páratlan fokú valós együtthatós polinomnak van valós gyöke.

Ötlet: párosítsunk minden gyököt a komplex konjugáltjával.

Gyök konjugáltja.

Állítás (Kiss-jegyzet, 3.3.6. Lemma)
Legyen $f = a_0 + a_1 x + \ldots + a_n x^n$ *valós* együtthatós polinom. Ha $c \in \mathbb{C}$ gyöke f-nek, akkor c konjugáltja is gyöke f-nek.

Bizonyítás

$$a_0 + a_1 c + \ldots + a_n c^n = 0,$$

vegyük mindkét oldal konjugáltját. A konjugálás összeg- és szorzattartó:

$$\overline{z+w} = \overline{z} + \overline{w} \text{ és } \overline{zw} = \overline{z}\,\overline{w}.$$

Így ezt kapjuk:

$$f\left(\overline{c}\right) = \overline{a_0} + \overline{a_1}\,\overline{c} + \ldots + \overline{a_n}\,\overline{c}^n = \overline{0} = 0.$$

Valós szám konjugáltja önmaga, tehát $\overline{0} = 0$ és $\overline{a_j} = a_j$. Így a bal oldalon $f\left(\overline{c}\right)$ áll, a jobb oldalon 0, tehát $\overline{c}$ gyöke f-nek. □

A konjugált multiplicitása.

Állítás
A c és a $\overline{c}$ *ugyanannyiszoros gyöke* f-nek.

Bizonyítás
f foka szerinti indukcióval. Ha c valós: nyilvánvaló. Legyen $c = a + bi$, ekkor $\overline{c} = a - bi$. Ha c nem valós, akkor $c \neq \overline{c}$, így $x - c$ és $x - \overline{c}$ egyszerre kiemelhetők. Tehát $f(x) = (x-c)(x-\overline{c})h(x)$, ahol $h \in \mathbb{C}[x]$.
$(x-c)(x-\overline{c}) = x^2 - (c+\overline{c})x + c\overline{c} = x^2 - 2ax + (a^2+b^2) \in \mathbb{R}[x]$.
A korábbi Következmény miatt $h(x)$ is valós együtthatós. Az indukciós feltevés miatt c és $\overline{c}$ ugyanannyiszoros, mondjuk k-szoros gyökei $h(x)$-nek ($k = 0$ is lehet!). Így $f(x)$-nek c és $\overline{c}$ is $k+1$-szeres gyöke. □