1. A maradékos osztás

Egész számok osztása

Példa

$$\begin{array}{r} 223 \,:\, 7 = \boxed{31} \\ \underline{-21} \\ 13 \\ \underline{-7} \\ \boxed{6} \end{array}$$

$223 = 7 \cdot 31 + 6$. Itt 31 a *hányados*, 6 a *maradék*.

Visszaszorzunk
Kivonunk

Állítás (kicsit gyengébb, mint 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

$$\begin{array}{r} (2x^3 + \ 2x^2 + 3x \ + 2) \ : \ (x^2 + 1) = \boxed{2x + 2} \\ \underline{-(2x^3 + \ \ 0 \ \ + 2x)} \\ 2x^2 + \ x \ + 2 \\ \underline{-\,(2x^2 + \ 0 \ + 2)} \\ \boxed{x} \end{array}$$

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

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

Tétel (K3.2.1)
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 *hányados* és r *maradék* ***egyértelműen*** meghatározott.

Maradékos osztás: létezés

Tétel (K3.2.1)
Legyen R szokásos gyűrű.
Ekkor az $R[x]$ polinomgyűrűben minden olyan $g \in R[x]$ polinommal lehet *maradékosan osztani*, amelynek *főegyüttható invertálható* (azaz egység).
Ez azt jelenti, hogy tetszőleges $f \in R[x]$ polinomhoz léteznek olyan $q, r \in R[x]$ polinomok, melyekre $f = gq + r$, ahol vagy $r = 0$, vagy r foka kisebb g fokánál.

Indukció $\mathrm{gr}(f)$ szerint. 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 invertálható, $m \leq n$. 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 $\mathrm{gr}(r) < \mathrm{gr}(g)$.
Visszahelyettesítve $f = f_0 + (a/b)x^{n-m}g = g\big(q_0 + (a/b)x^{n-m}\big) + r$. Tehát f is eloszthető maradékosan g-vel. □

Maradékos osztás: együtthatók

Következmény
Test fölött, speciálisan $\mathbb{C}[x]$-ben, $\mathbb{R}[x]$-ben és $\mathbb{Q}[x]$-ben minden nem nulla polinommal lehet maradékosan osztani.
Oka: A nem nulla főegyüttható invertálható. $\mathbb{Z}[x]$-ben oszthatunk maradékosan az olyan polinomokkal, *amelyek főegyütthatója egység $\mathbb{Z}$-ben, azaz* 1 *vagy* -1.

Példa (K3.2.18)
Az $x : 2$ maradékos osztás nem végezhető el $\mathbb{Z}[x]$-ben.

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. □

Maradékos osztás: egyértelműség

Tétel (K3.2.1)
$f, g \in R[x]$, ahol g főegyütthatója invertálható (elég, hogy $g \neq 0$).
$f = gq_1 + r_1$, 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 $r_1 = r_2$.

$gq_1 + r_1 = f = gq_2 + r_2$, 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 $\mathrm{gr}\big(g(q_1 - q_2)\big) = \mathrm{gr}(g) + \mathrm{gr}(q_1 - q_2) \geq \mathrm{gr}(g)$. Tehát a bal oldal foka nagyobb a jobb oldal fokánál: ellentmondás.
Ezért $q_1 - q_2 = 0$, és így $q_1 = q_2$. De akkor $r_2 - r_1 = g \cdot 0 = 0$, és így $r_1 = r_2$. □
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 $x/2 \notin \mathbb{Z}[x]$.

Euklideszi gyűrű
A maradékos osztás tételében nemcsak a négy alapművelet szerepel, hanem egészek esetében az abszolút érték, polinomoknál a fokszám. Ezek közös általánosítása a következő.

Definíció (K5.5.1)
Az R szokásos gyűrűt *euklideszi gyűrűnek* nevezzük, ha R nem nulla elemein értelmezve van egy nemnegatív egész értékű φ függvény (az úgynevezett *euklideszi norma*) a következő tulajdonsággal. Minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy $a = bq + r$ és $r = 0$ vagy $\varphi(r) < \varphi(b)$.

Az egészek gyűrűje euklideszi, φ az *abszolút érték.*
Test fölötti polinomgyűrű euklideszi, φ a *fokszám.*
Látni fogjuk, hogy euklideszi gyűrűben érvényes a számelmélet alaptétele.
$\mathbb{Z}[x]$-ben is, de itt nemcsak a fokszámra nézve nem lehet elvégezni a maradékos osztást, hanem más φ-re sem (K5.5.7).

2. Számelmélet gyűrűkben

Oszthatóság

Definíció (K3.1.3)
Az R *szokásos* gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük.
Ha $r, s \in R$, akkor r *osztója* s-nek (s *többszöröse* r-nek), ha van olyan $t \in R$, hogy $rt = s$. Jele: $r \mid s$.

Példa: $2x \mid 3x^2$ igaz $\mathbb{R}[x]$-ben, nem igaz $\mathbb{Z}[x]$-ben.

Tulajdonságok (K3.1.4)

(1) Ha $r \mid s$ és $r \mid t$, akkor $r \mid s \pm t$.

(2) Ha $r \mid s$, akkor $r \mid st$, sőt $rt \mid st$. Megfordítva, ha $t \neq 0$, akkor $rt \mid st$-ből $r \mid s$ következik (R nullosztómentes!).

(3) *Tranzitivitás*: ha $r \mid s$ és $s \mid t$, akkor $r \mid t$.

(4) *Reflexivitás*: $r \mid r$ minden $r \in R$ esetén (R egységelemes!).

Felbonthatatlan elem

Emlékeztető (K3.1.7, 3.1.9)
Az $e \in R$ *egység*, ha $e \mid 1$. Ez ugyanaz, mint az invertálható elem. Minden egység osztója R minden elemének.
Az $a, b \in \mathbb{R}$ *asszociáltak*, ha $a \mid b$ és $b \mid a$. Ez azzal ekvivalens, hogy egymás egységszeresei.

Vigyázzunk, *az egység és az egységelem nem ugyanaz a fogalom!*
Példa: A $\mathbb{Z}$ gyűrű egységei ± 1. Az egység*eleme* az 1.

Definíció (K3.1.12, K3.1.13, K3.1.14)
A $b = cd$ a b-nek *triviális* felbontása, ha c és d egyike egység.
A $p \in R$ *felbonthatatlan* (irreducibilis), ha nem nulla, nem egység,
és *nincs nemtriviális felbontása.*
Ekvivalens: p minden osztója egység, vagy p egységszerese.

Példa: $\mathbb{R}[x]$-ben $x = (3/2)(2x/3)$ az x-nek egy triviális felbontása.

Alaptételes gyűrű, prím, KKO

Definíció (K3.1.15, 3.1.25, 3.1.19)
Az R gyűrűben *érvényes a számelmélet alaptétele*, ha R minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve *egyértelműen* felbontható felbonthatatlan elemek szorzatára.
Az ilyen gyűrűt *alaptételes* gyűrűnek nevezzük.

A $b, c \in R$ elemeknek d *kitüntetett közös osztója*, ha

(1) közös osztó, azaz $d \mid b$ és $d \mid c$;

(2) minden közös osztónak többese: $d' \mid b$ és $d' \mid c \implies d' \mid d$.

A $p \in R$ *prím* R-ben, ha nem nulla, nem egység, és tetszőleges $b, c \in R$ esetén $p \mid bc$-ből következik, hogy $p \mid b$ vagy $p \mid c$.

Az alaptétel bizonyítása

Tétel (K5.5.9)
Ha R euklideszi gyűrű akkor az euklideszi algoritmus miatt bármely két elemnek van kitüntetett közös osztója, és érvényes a kitüntetett közös osztó kiemelési tulajdonsága.

Állítás (K3.1.27)
Ha egy szokásos gyűrűben bármely két elemnek van kitüntetett közös osztója, akkor a felbonthatatlanok prímek.

Tétel (K3.2.12, 5.5.9)
Minden euklideszi gyűrű alaptételes.

A bizonyítások csaknem betűről betűre megegyeznek azokkal a gondolatmenetekkel, amiket egészekre láttunk. □

Kanonikus alak

Definíció (K3.1.16)
A $0 \neq r$ *kanonikus alakja* $r = ep_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, ahol e egység, $p_1, p_2, \dots, p_k$ pedig felbonthatatlanok, amelyek páronként nem asszociáltak.

Példák
$\mathbb{Z}$-ben $-36 = (-1)2^2 3^2$.
$\mathbb{C}[x]$-ben $f(x) = c(x-b_1)^{k_1}(x-b_2)^{k_2}\dots(x-b_m)^{k_m}$,
ahol a c a főegyüttható (nem nulla konstans, így egység). Ez a gyöktényezős alak, a k_i a b_i gyök multiplicitása.

Az *osztók száma*, a *kitüntetett közös osztó*, és a kitüntetett közös többszörös hasonló képletekkel kapható a kanonikus alakból, mint az egész számok számelméletében.

Kongruenciák euklideszi gyűrűben
Euklideszi gyűrűben érvényesek a kongruenciákról tanultak is:

- A lineáris diofantikus egyenletek megoldhatósága.
- A kongruenciák értelmezése és alaptulajdonságai.
- A maradékosztály fogalma.
- A lineáris és szimultán kongruenciarendszerek megoldhatósága.
- A kínai maradéktétel.

Ez utóbbit most illusztráljuk az interpoláció témaköre kapcsán.

Legyen T test. Ha $a_1, \dots, a_n \in T$ páronként különböző, akkor $x - a_i$ páronként relatív prímek (bármely kettő különbsége egység).
Így a kínai maradéktétel miatt minden $b_1, \dots, b_n \in T$-hez van olyan $f(x) \in T[x]$, melyre $f(x) \equiv b_i \ (x - a_i) \ (1 \leq i \leq n)$.
Ez azt jelenti, hogy $x - a_i \mid f(x) - b_i$, vagyis alkalmas g_i-re
$f(x) - b_i = g_i(x)(x - a_i)$, és a_i-t helyettesítve $f(a_i) = b_i$.

3. Interpoláció

Az interpoláció alapproblémája

Feladat
Olyan polinomot keresünk, amely *előre megadott helyeken előre megadott értékeket* vesz fel.
A *helyek*: páronként különböző $a_1, a_2, \dots, a_n$ számok.
Az *értékek*: tetszőleges $b_1, b_2, \dots, b_n$ számok.
Azt szeretnénk: $f(a_1) = b_1, f(a_2) = b_2, \dots, f(a_n) = b_n$.

Az interpoláció tétele
Mindig pontosan egy ilyen f polinom van a legfeljebb $n-1$-edfokú polinomok között (a nullapolinomot is ideértve).

Az interpolációs polinom létezését láttuk az imént, de fogunk mutatni két konkrét konstrukciós módszert is.
Egyértelműség: Ha f és g ilyen polinomok, akkor n helyen megegyeznek, így a polinomok azonossági tétele miatt egyenlők. □

Lagrange konstrukciója

Lagrange-interpoláció (K2.4.12)
Keressünk először ilyet: $\ell_1(a_1) = 1, \ell_1(a_2) = 0, \ldots, \ell_1(a_n) = 0$. Az ℓ_1 polinomnak tehát $a_2, \ldots, a_n$ gyöke. Ezért legyen $\ell_1(x) = c(x-a_2)\ldots(x-a_n)$, ahol $c \in \mathbb{C}$. A c értékét az a_1 behelyettesítésével határozhatjuk meg:

$$\ell_1(x) = \frac{(x-a_2)\ldots(x-a_n)}{(a_1-a_2)\ldots(a_1-a_n)}\,.$$

Analóg módon létezik $\ell_j(x)$ minden $2 \le j \le n$-re, melyre $\ell_j(a_j) = 1$, és a többi a_k gyöke ℓ_j-nek (ha $k \neq j$).
Jó lesz: $f(x) = b_1\ell_1(x) + b_2\ell_2(x) + \ldots + b_n\ell_n(x)$.
Például $f(a_1) = b_1\ell_1(a_1) + b_2\ell_2(a_1) + \ldots + b_n\ell_n(a_1) =$
$= b_1 \cdot 1 + b_2 \cdot 0 + \ldots + b_n \cdot 0 = b_1$.
Hasonlóan látható, hogy $f(a_2) = b_2, \ldots, f(a_n) = b_n$. □

Newton-interpoláció
Megfordítva, a kínai maradéktétel FGy2.6.2-beli második bizonyítása a Lagrange-interpoláció ötletén alapszik.

A Lagrange-interpoláció hátránya
Képzeljük, hogy a $b_1, \ldots, b_n$ számok *mérési eredmények*. Kiszámítjuk Lagrange módszerével az interpolációs polinomot: $f(a_1) = b_1, f(a_2) = b_2, \ldots, f(a_n) = b_n$. Keletkezik egy új mérési eredmény: az a_{n+1} helyen b_{n+1}. Ekkor sajnos előlről kell kezdeni a számolást. A megoldás: a *Newton-interpoláció* (K2.4.13).
Az $a_1, \ldots, a_n$ helyeken megfelelő f polinomhoz egy

$$g(x) = c(x-a_1)(x-a_2)\ldots(x-a_n)$$

alakú korrekciós tagot adunk hozzá. Ez nem rontja el az $a_1, \ldots, a_n$ helyeken felvett értékeket. A c-t úgy választjuk, hogy az $f+g$ az a_{n+1} helyen is jó legyen. □

4. Összefoglaló

A 22. előadáshoz tartozó vizsgaanyag

Fogalmak
Oszthatóság (K3.1.3), asszociált (K3.1.7), egység (K3.1.9), triviális felbontás, felbonthatatlan elem (K3.1.12–14).
Kitüntetett közös osztó (K3.1.19), prím (3.1.25), alaptételes és euklideszi gyűrű (K3.1.15, 3.1.25, 5.5.1). Kanonikus alak (K3.1.16).

Tételek
Maradékos osztás szokásos gyűrű fölötti polinomokra: létezés
és egyértelműség (K3.2.1).
$\mathbb{Z}[x]$-ben nincs maradékos osztás (K3.2.18), nem is euklideszi (K5.5.7).
Az oszthatóság tulajdonságai (K3.1.4).
A KKO létezése és kiemelési tulajdonsága euklideszi gyűrűben (K5.5.9).
Ha van KKO, akkor minden irreducibilis prím (K3.1.27).
Euklideszi gyűrű alaptételes (K3,2,12, 5.5.9).
Lagrange- és Newton-interpoláció, egyértelműség (K2.4.10–13).