1. A maradékos osztás

Egész számok osztása

Példa

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

$223 = 7 \cdot 31 + 6.$

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

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

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

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

Tétel (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 és r egyértelműen meghatározott.

Maradékos osztás: létezés

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 $\mathrm{gr}(r) < \mathrm{gr}(g)$.

Bizonyítás
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 $b \neq 0$ 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 eloszthető maradékosan g-vel. □

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

Maradékos osztás: együtthatók

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 (K3.2.18)
Az $x : 2$ 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 (K3.2.1)
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 $\mathrm{gr}\big(g(q_1 - q_2)\big) = \mathrm{gr}(g) + \mathrm{gr}(q_1 - q_2) \geq \mathrm{gr}(g)$. 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 $r_1 = r_2$. □

2. Oszthatóság polinomok között

Oszthatóság

Definíció (K3.1.3)
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 $h(x) = c_0 + c_1 x + \ldots$, és $c_0, c_1, \ldots$ egészek, akkor x együtthatóját véve $2c_1 = 1$ teljesülne.

A hányados együtthatói

Következmény (K3.2.2)
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 (K3.1.9)
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.

Állítás (K3.1.11)
$\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ 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 (K3.1.19)
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 (K3.1. és K3.2. 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 (K2.5. szakasz)
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 (K3.3.9)
Páratlan fokú valós együtthatós polinomnak van valós gyöke.

Ötlet: párosítsunk minden gyököt a komplex konjugáltjával.

Gyök konjugáltja

Állítás (K3.3.6)
Legyen $f = a_0 + a_1x + \ldots + a_nx^n$ *valós* együtthatós polinom. Ha $c \in \mathbb{C}$ gyöke f-nek, akkor c konjugáltja is gyöke f-nek.

Bizonyítás

$$a_0 + a_1c + \ldots + a_nc^n = 0,$$

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:

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

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

A konjugált multiplicitása

Állítás (K3.3.6)
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 (K3.2.2) 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. □

4. Polinomok számelmélete

Polinomok szorzatra bontása

Cél
Polinomok szorzatra bontása, ameddig csak lehetséges. Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$. Itt 2 és 3 *felbonthatatlan*, azaz irreducibilis számok.

Definíció-kísérlet
Egy polinomot nevezzünk *irreducibilisnek* (felbonthatatlannak), ha nem lehet szorzatra bontani.

Problémák

(1) Az x irreducibilis? $x = 1 \cdot x = (-1)(-x) = (1/2)(2x)$. Ugyanígy $2 = 1 \cdot 2$, de a 2 mégis felbonthatatlan szám.

(2) $x^2 + 1 = (x + i)(x - i)$ valós fölött nem bontható föl. Akkor most $x^2 + 1$ irreducibilis-e, vagy sem?

Felbonthatatlan számok

Emlékeztető számelméletből
Az egész számok között az *egységek*: 1 és -1. Az n szám *triviális felbontása* $n = ab$, ha a vagy b egység. Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$. Az n szám *felbonthatatlan*, ha nincs nemtriviális felbontása. A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.
Példa: A 2 számnak csak triviális felbontásai vannak. Mivel 2 nem egység, ezért a 2 felbonthatatlan.

A számelmélet alaptétele: minden nullától és egységtől különböző szám *felírható* felbonthatatlanok szorzataként. Ez *egyértelmű*, ha a sorrendtől és egységszerestől eltekintünk. A bizonyítás fő eszköze: a *kitüntetett közös osztó*.

Irreducibilis polinomok

Definíció (K3.1.12, K3.1.13)
Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike.
Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása *triviális* ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben. Az $f \in R[x]$ polinom *irreducibilis* $R[x]$-ben (R fölött), ha *nincs nemtriviális felbontása*, és nem egység. *Reducibilis* azt jelenti: nem egység és nem irreducibilis.

A számelmélet alaptétele polinomokra (K3.2.12, K3.4.10)
Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike.
Minden nullától és egységtől különböző $R[x]$-beli polinom *felírható* $R[x]$-beli irreducibilisek szorzataként. Ez *egyértelmű*, ha a sorrendtől és egységszerestől eltekintünk.

Bizonyítás: $\mathbb{C}, \mathbb{R}, \mathbb{Q}$-ra mint számelméletből, $\mathbb{Z}[x]$-re később.

Példák felbontásra

Példa (K3.3.14)
Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:
$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

$\mathbb{R}[x]$-ben 3 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 + 1)$$

$\mathbb{Q}[x]$-ben 2 tényező:

$$(6x^2 - 12) \cdot (x^2 + 1)$$

$\mathbb{Z}[x]$-ben 4 tényező:

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

Tanulság
A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység. A $\mathbb{Z}[x]$-ben 6 nem egység, sőt 2, 3 itt irreducibilis polinomok.

Az alaptétel bizonyítása

Az alaptétel bizonyítása
$\mathbb{C}, \mathbb{R}, \mathbb{Q}$ fölött ugyanúgy, mint egész számokra (K3.2.13, K3.2.14):

(1) Az euklideszi algoritmus miatt bármely két polinomnak van *kitüntetett közös osztója*.

(2) Erre teljesül a *kiemelési tulajdonság*: $(fg, fh) = f(g, h)$ (lásd K3.1.23.)

(3) Emiatt minden irreducibilis f polinom *prímtulajdonságú*: ha $f \mid gh$, akkor $f \mid g$ vagy $f \mid h$. (lásd K3.1.25.)

(4) Ebből következik az alaptétel *egyértelműségi* állítása (ugyanúgy, mint egész számokra).

(5) A felbontás *létezése* fokszám szerinti indukcióval.

A $\mathbb{Z}[x]$-beli alaptételt a $\mathbb{Q}[x]$-beli alaptételre vezetjük vissza (K3.4. szakasz).

5. Az irreducibilitás eldöntése

Gyökök és irreducibilitás

Tétel (K3.3. Szakasz)
Legyen T a $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ egyike.

(1) Az $f \in T[x]$ akkor és csak akkor irreducibilis T fölött, ha nem konstans, és nem bontható $T[x]$-ben *alacsonyabb fokú* polinomok szorzatára.

(2) *Elsőfokú* polinom mindig irreducibilis $T[x]$-ben.

(3) *Másod- és harmadfokú* polinom akkor és csak akkor irreducibilis $T[x]$-ben, ha *nincs gyöke* T-ben.

(4) *Legalább negyedfokú* polinom, *HA* van gyöke T-ben, akkor biztosan *NEM* irreducibilis $T[x]$-ben.
Ha nincs gyöke, attól még lehet reducibilis! Példa: $\mathbb{Q}[x]$-ben $(x^2+1)^2$.

(5) Gyök létezése *elsőfokú* irreducibilis tényezőnek felel meg.

Ezek közül csak (4) igaz $\mathbb{Z}[x]$-ben!

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel (K3.3.5)
A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás
Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$. Ezért g és h egyike nulladfokú, és így egység.

Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú. Az *algebra alaptétele* miatt van f-nek egy $c \in \mathbb{C}$ gyöke. Ekkor $f(x) = (x-c)h(x)$ alkalmas $h \in \mathbb{C}[x]$-re. Ez a felbontás triviális kell legyen, és ezért h egység. Tehát f tényleg elsőfokú. □

Egy komplex együtthatós polinom irreducibilisekre való felbontását úgy kapjuk, hogy gyöktényezőkre bontjuk, és a főegyütthatót valamelyik tényezőhöz hozzácsapjuk.

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel (K3.3.8)
Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)
Ha $f \in \mathbb{R}[x]$ legalább elsőfokú, akkor az *algebra alaptétele* miatt van c komplex gyöke. Ha c valós, $x-c$ kiemelhető $\mathbb{R}$ fölött. Ha nem, láttuk korábban:
$(x-c)(x-\overline{c})$ valós együtthatós, és $f(x)$-ből kiemelhető, ami $\mathbb{R}$ fölötti felbontást ad. Ezért ha f irreducibilis $\mathbb{R}$ fölött, akkor legfeljebb másodfokú.

Egy valós együtthatós polinom irreducibilisekre való felbontását úgy kapjuk, hogy gyöktényezőkre bontjuk $\mathbb{C}$ fölött, és mindegyik nem valós gyököt párosítjuk a komplex konjugáltjával.
Példa: $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$ (K2.5.10. Gyakorlat).

Irreducibilitás $\mathbb{Q}[x]$-ben (K3.5. szakasz)

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a *racionális gyökteszt* segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (K3.5.2)
Legyen f egész együtthatós, nem konstans polinom. *HA* van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis $\mathbb{Q}$ fölött.

Példa: $21x^4 + 60x - 150$ irreducibilis $\mathbb{Q}$ fölött ($p = 2$ jó). A $p = 3$ nem jó: $3 \mid 21$. A $p = 5$ nem jó: $5^2 \mid 150$.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) *Nem igaz a megfordítása.* Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és *nem* $\mathbb{Z}$ fölötti irreducibilitást biztosít. Példa: $9x + 18$ irreducibilis $\mathbb{Q}$ fölött, de $\mathbb{Z}$ fölött nem.

(4) A kritérium miatt $x^n - 2$ irreducibilis minden $n \geq 1$-re. Azaz *létezik* $\mathbb{Q}$ *fölött akárhányadfokú irreducibilis polinom.*

(5) Fordított Schönemann–Eisenstein-kritérium: Ha a p prím osztja a polinom minden együtthatóját a konstans tag kivételével, és p^2 nem osztja a főegyütthatót, a polinom akkor is irreducibilis $\mathbb{Q}$ fölött (K3.5.7).

További módszerek $\mathbb{Q}$ fölött

Állítás (K3.5.5)
$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas *eltoltja*, vagyis az $f(x + c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

Példa
$x^4 + 1$-re nem alkalmazható a Schönemann–Eisenstein.
$(x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, erre már igen, $p = 2$-vel. Tehát $x^4 + 1$ is irreducibilis $\mathbb{Q}$ fölött.

Tétel
Létezik algoritmus az irreducibilitás eldöntésére $\mathbb{Q}$ fölött, például interpoláció segítségével. Van hatékony algoritmus is.

A módszerek összefoglalása: a Kiss-könyv 111. oldalán.

6. Egész együtthatós polinomok

Primitív polinomok

Emlékeztető
Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Kiemeltük az együtthatók legnagyobb közös osztóját.

Definíció (K3.4.1)
Primitív polinom: együtthatóinak legnagyobb közös osztója 1.

Állítás
Minden egész együtthatós polinom egyértelműen fölírható egy primitív polinom, és egy egész szám szorzataként.

Példa: $60x^6 + 36x^4 + 90 = 6(10x^6 + 6x^4 + 15)$. Nyilván $(10, 6, 15) = 1$ (de nem páronként relatív prímek).

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (K3.4.8)
Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Az $f \in \mathbb{Z}[x]$ polinomot a következőképpen bonthatjuk $\mathbb{Z}$ fölött irreducibilisek szorzatára:

(1) Kiemeljük az együtthatóinak a legnagyobb közös osztóját: $f(x) = ng(x)$, ahol g már primitív polinom;

(2) Az n számot $\mathbb{Z}$-ben prímek szorzatára bontjuk;

(3) A g polinomot $\mathbb{Q}[x]$-ben bontjuk irreducibilisek szorzatára.

Meg lehet mutatni, hogy g felbontása is „lényegében" egész együtthatós polinomokra történik (II. Gauss-lemma, K3.4.7).

7. Összefoglaló

A 9. előadáshoz tartozó vizsgaanyag

Fogalmak
Oszthatóság, egység, triviális felbontás, irreducibilis polinom. Kitüntetett közös osztó. Primitív polinom.

Tételek
Maradékos osztás polinomokra: létezés és egyértelműség. A hányados és a maradék együtthatói összeadás, kivonás, szorzás, és az osztó főegyütthatójával való osztás segítségével kaphatók. Az egységek leírása a polinomok között. A kitüntetett közös osztó létezése, $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ alaptételes. Páratlan fokú valós együtthatós polinomnak van valós gyöke. Konjugált gyök multiplicitása valós együtthatós polinomra. Gyökök és irreducibilitás kapcsolata. A $\mathbb{C}[x]$ és $\mathbb{R}[x]$ irreducibilisei. A Schönemann–Eisenstein-kritérium. Az eltolt irreducibilitása. A $\mathbb{Z}[x]$ irreducibiliseinek visszavezetése $\mathbb{Q}[x]$-re, $\mathbb{Z}[x]$ alaptételes.