1. A számelmélet alapjai polinomok között

Oszthatóság

Ismétlés (K3.1.3, K2.3.2)
Legyen R szokásos gyűrű. A $g \in R[x]$ *osztója* $f \in R[x]$-nek $R[x]$-ben, ha létezik olyan $h \in R[x]$, hogy $f(x) = g(x)h(x)$. Jelölés: $g \mid f$ (vagy néha $g \mid_{R[x]} f$). Az $f \in R[x]$ polinom pontosan akkor egység, ha egy olyan konstans polinom, amely egység R-ben.

$x + 1$ 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 (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.

2. Irreducibilis polinomok

Példák felbontásra

Ismétlés (K3.1.13)
Legyen R szokásos gyűrű. Az $f \in R[x]$ polinom *irreducibilis R fölött*, ha nem nulla, nem egység, és ha $f = gh$, ahol $g, h \in R[x]$, akkor g és h valamelyike egység (azaz konstans, és R-ben egység).

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

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.

Gyökök és irreducibilitás

Tétel (K3.3. szakasz)
Legyen T test.

(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!

Gyökök és irreducibilitás — bizonyításvázlat

Legyen T test. Ekkor egy $g \in T[x]$ polinom *pontosan akkor egység, ha* nem 0 konstans, azaz *a foka* 0.

Ha $f = gh$, akkor $\mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$. Ezért ez a felbontás akkor és csak akkor nemtriviális, ha $0 < \mathrm{gr}(g), \mathrm{gr}(h) < \mathrm{gr}(f)$. Így f *akkor reducibilis, ha alacsonyabb fokúak szorzatára bomlik.*

Ha $\mathrm{gr}(f) = 1$, akkor ez nem lehetséges, és f nem is egység. Ezért *elsőfokú polinom mindig irreducibilis.*

Ha f-nek van egy $c \in T$ gyöke, akkor az $x - c$ gyöktényező kiemelhető, és ezért f-nek van elsőfokú tényezője T fölött. Megfordítva, ha $f = gh$, és például g foka 1, akkor $g(x) = ax + b$ alakú, ezért $-b/a \in T$ gyöke g-nek, így f-nek is. Tehát *gyök létezése tényleg elsőfokú tényezőnek felel meg.*

Ha $\mathrm{gr}(f) = 2$ vagy 3, és $f = gh$ nemtriviális felbontás, akkor $\mathrm{gr}(g)$ és $\mathrm{gr}(h)$ valamelyike 1, és ezért f-nek van gyöke T-ben. □

Irreducibilitás $\mathbb{C}[x]$-ben

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

Bizonyítás
Ha f elsőfokú, akkor irreducibilis (láttuk).
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.

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:

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

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

A konjugált multiplicitása

Állítás (K3.3.6)
Ha $f \in \mathbb{R}[x]$, akkor 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. □

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
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).

4. Összefoglaló

A 23. előadáshoz tartozó vizsgaanyag

Fogalmak
Egység és irreducibilitás a polinomgyűrűben (K3.1.3, 2.3.2, 3.1.13).

Tételek
Gyökök és irreducibilitás kapcsolata test fölött (K3.3).
Páratlan fokú valós együtthatós polinomnak van valós gyöke (K3.3.9).
Konjugált gyök multiplicitása valós együtthatós polinomra (K3.3.6).
A $\mathbb{C}[x]$ és $\mathbb{R}[x]$ irreducibilisei (K3.3.5, 3.3.8).