Diszkrét matematika 2.C szakirány

7. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼nagy

Komputeralgebra Tanszék

2016. ősz

Polinomok felbonthatósága

Definíció

Legyen R egységelemes integritási tartomány.
Ha a $0 \neq f \in R[x]$ polinom nem egység, akkor felbonthatatlannak (irreducibilisnek) nevezzük, ha $\forall a, b \in R[x]$-re

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

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-előállítása (olyan, amiben egyik tényező sem egység).

Polinomok felbonthatósága

Állítás

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

Bizonyítás

$0 \circ r = (0 * 0) \circ r = (0 \circ r) * (0 \circ r) \Longrightarrow 0 = 0 \circ r$.
A másik állítás bizonyítása ugyanígy.

Állítás

Test nullosztómentes.

Bizonyítás

Legyen $(F; *, \circ)$ test $0 \in F$ nullelemmel, és $1 \in F$ egységelemmel.
Indirekt tfh. léteznek $a, b \in F$ nem-nulla elemek, amikre $a \circ b = 0$.
Ekkor $b = 1 \circ b = a^{-1} \circ a \circ b = a^{-1} \circ 0 = 0$, ami ellentmondás.

Polinomok felbonthatósága

Állítás

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

Bizonyítás

$\Longleftarrow$

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 $f_0 \cdot f_0^{-1} = 1$, így f tényleg egység.

$\Longrightarrow$

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

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 $f(x) = f_1 x + f_0$ alakban, ahol $f_1 \neq 0$. Azt szeretnénk, hogy létezzen $c \in F$, amire $f(c) = 0$, vagyis $f_1 c + f_0 = 0$. Ekkor $f_1 c = -f_0$ (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. $2x - 1 \in \mathbb{Z}[x]$.

Polinomok felbonthatósága

Állítás

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

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

$\Longleftarrow$

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

$\Longrightarrow$

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

Tétel

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

Bizonyítás

$\Longleftarrow$

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

$\Longrightarrow$

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.

Polinomok felbonthatósága

Tétel

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

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

Bizonyítás

$\Longleftarrow$

Ha $deg(f) = 1$, akkor korábbi állítás alapján f felbonthatatlan.
Ha $deg(f) = 2$, és f-nek nincs gyöke, akkor f nem áll elő két elsőfokú polinom szorzataként (Miért?), vagyis csak olyan kéttényezős szorzat-előállítása lehet, melyben az egyik tényező foka 0, tehát egység.

$\Longrightarrow$

Ha f felbonthatatlan, akkor nem lehet $deg(f) < 1$. (Miért?)
Ha f felbonthatatlan, és $deg(f) = 2$, akkor tfh. van gyöke. Ekkor az ehhez tartozó gyöktényező kiemelésével egy nemtriviális felbontását kapjuk f-nek (Miért?), ami ellentmondás.

Polinomok felbonthatósága

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 $g(x) = (x - c)(x - \overline{c}) = x^2 - 2\,\mathrm{Re}(c)x + |c|^2 \in \mathbb{R}[x]$ 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 $\overline{c}$ is gyöke, hiszen

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

Polinomok felbonthatósága

Definíció

$f \in \mathbb{Z}[x]$-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 $f_0 g_{i+j} + \ldots + f_i g_j + \ldots + f_{i+j} g_0$, 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

Állítás

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

Állítás

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

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 előállítása 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

Következmény

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

Bizonyítás

$\Longrightarrow$

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

$\Longleftarrow$

A Gauss-tételből következik az állítás.

Polinomok felbonthatósága

Tétel (Schönemann-Eisenstein)

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

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

akkor f felbonthatatlan $\mathbb{Z}$ fölött.