

Diszkrét matematika II.

7. előadás

Fancsali Szabolcs Levente
nudniq@inf.elte.hu

ELTE IK Komputeralgebra Tanszék

Mérai László diái alapján

Polinomok felbonthatósága

Definíció

Legyen R egységelemes integritási tartomány, és legyen $0 \neq f \in R[x]$ polinom nem egység.

Ezt az f nemnulla polinomot pontosan akkor nevezzük **felbonthatatlannak** (irreducibilisnek), ha $\forall a, b \in R[x]$ -re

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

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).

A konstans nulla polinomot sem felbonthatatlannak, sem felbonthatónak nem nevezzük.

Polinomok felbonthatósága

Állítás

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

Bizonyítás

\Leftarrow

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.

\Rightarrow

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 $f(x) = f_1x + f_0$ alakban, ahol $f_1 \neq 0$. Azt szeretnénk, hogy létezzen $c \in F$, amire $f(c) = 0$, vagyis $f_1c + f_0 = 0$. Ekkor $f_1c = -f_0$ (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. $2x - 1 \in \mathbb{Z}[x]$ polinomnak nincs egész gyöke. (És emlékezzünk, hogy $R[x]$ -beli polinomnak csak R -beli gyökeit definiáltuk. . .)

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



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



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



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



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.

Az algebra alaptételét itt használtuk, de nem bizonyítottuk!

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



Ha $\deg(f) = 1$, akkor korábbi állítás (test fölötti elsőfokú polinom...) alapján f felbonthatatlan.

Ha $\deg(f) = 2$, és f -nek nincs gyöke, akkor korábbi állítás (test fölötti másodfokú polinom...) alapján f felbonthatatlan.



Ha f felbonthatatlan, akkor nem lehet $\deg(f) < 1$. (Miért?)

Ha f felbonthatatlan, és $\deg(f) = 2$, akkor nem lehet gyöke. (Miért?)

De még nem vagyunk kész! Még nem láttuk, hogy ne lehetne kettőnél magasabb fokú egy \mathbb{R} felett irreducibilis polinom.

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

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

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

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 $f_0g_{i+j} + \dots + f_i g_j + \dots + f_{i+j}g_0$, 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.

A felírás lényegében egyértelmű.

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.

A felírás lényegében egyértelmű.

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 előállítására 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

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

Bizonyítás

\Rightarrow

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

\Leftarrow

A Gauss-tételből következik az állítás.

Polinomok felbonthatósága

Tétel (Schönemann-Eisenstein)

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

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

akkor f felbonthatatlan \mathbb{Z} fölött.

Bizonyítás

Tfh. $f = gh$. Mivel p nem osztja f főegyütthatóját, ezért sem a g , sem a h főegyütthatóját nem osztja (Miért?). Legyen m a legkisebb olyan index, amelyre $p \nmid g_m$, és o a legkisebb olyan index, amelyre $p \nmid h_o$. Ha $k = m + o$, akkor

$$p \nmid f_k = \sum_{i+j=k} g_i h_j,$$

mivel p osztja az összeg minden tagját, kivéve azt, amelyben $i = m$ és $j = o$.

Polinomok felbonthatósága

Megjegyzések

- A feltételben f_n és f_0 szerepe felcserélhető.
- A tétel nem használható test fölötti polinom irreducibilitásának bizonyítására, mert testben nem léteznek prímek, hiszen minden nem-nulla elem egység.

Racionális gyökteszt

Tétel

Legyen $f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ primitív polinom. Ha $f\left(\frac{p}{q}\right) = 0$, $p, q \in \mathbb{Z}$, $(p, q) = 1$, akkor $p|f_0$ és $q|f_n$.

Bizonyítás

$$0 = f\left(\frac{p}{q}\right) = f_n \left(\frac{p}{q}\right)^n + f_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + f_1 \left(\frac{p}{q}\right) + f_0 \quad / \cdot q^n$$

$$0 = f_n p^n + f_{n-1} q p^{n-1} + \dots + f_1 q^{n-1} p + f_0 q^n$$

$p|f_0 q^n$, mivel az összes többi tagnak osztója p , és így $(p, q) = 1$ miatt $p|f_0$.

$q|f_n p^n$, mivel az összes többi tagnak osztója q , és így $(p, q) = 1$ miatt $q|f_n$.

Megjegyzés

f primitívsege nem szükséges feltétel, csak praktikus. (Miért?)

A racionális gyökteszt alkalmazása

Állítás

$$\sqrt{2} \notin \mathbb{Q}.$$

Bizonyítás

Tekintsük az $x^2 - 2 \in \mathbb{Z}[x]$ polinomot.

Ennek a $\frac{p}{q}$ alakú gyökeire $(p, q \in \mathbb{Z}, (p, q) = 1)$ teljesül, hogy $p|2$ és $q|1$, így a lehetséges racionális gyökei ± 1 és ± 2 .

Véges testek

Tekintsük valamely p prímre a \mathbb{Z}_p testet, továbbá egy $f(x) \in \mathbb{Z}_p[x]$ felbonthatatlan főpolinomot. Vezessük be a $g(x) \equiv h(x) \pmod{f(x)}$, ha $f(x) | g(x) - h(x)$ relációt.

Ez ekvivalenciareláció, ezért meghatároz egy osztályozást $\mathbb{Z}_p[x]$ -en.

Minden osztálynak van $\deg(f)$ -nél alacsonyabb fokú reprezentánsa (Miért?), és ha $\deg(g), \deg(h) < \deg(f)$, továbbá g és h ugyanabban az osztályban van, akkor egyenlőek (Miért?). Tehát $\deg(f) = n$ esetén bijekciót létesíthetünk az n -nél kisebb fokú polinomok és az osztályok között, így p^n darab osztály van.

Az osztályok között értelmezhetjük a természetes módon a műveleteket. Ezeket végezhetjük az n -nél alacsonyabb fokú reprezentánsokkal: ha a szorzat foka nem kisebb, mint n , akkor az $f(x)$ -szel vett osztási maradékot vesszük.

Véges testek

$f \nmid g$ esetén a bővített euklideszi algoritmus alapján

$$d(x) = u(x)f(x) + v(x)g(x).$$

Mivel $f(x)$ felbonthatatlan, ezért $d(x) = d$ konstans polinom, így $\frac{v(x)}{d}$ multiplikatív inverze lesz $g(x)$ -nek.

Tétel (NB)

Az ekvivalenciaosztályok halmaza a rajta értelmezett összeadással és szorzással testet alkot.

Megjegyzés

Tetszőleges p prím és n pozitív egész esetén létezik p^n elemű test, mert létezik n -ed fokú felbonthatatlan polinom \mathbb{Z}_p -ben.

Megjegyzés

Véges test elemszáma prímszám, továbbá az azonos elemszámú testek izomorfak.

Véges testek

Példa

Tekintsük az $x^2 + 1 \in \mathbb{Z}_3[x]$ felbonthatatlan polinomot (Miért az?). A legfeljebb elsőfokú polinomok: $0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$. Az összeadás műveleti táblája:

+	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1

Például:

$$2x + 2 + 2x + 1 = 4x + 3 \stackrel{\mathbb{Z}_3}{=} x$$

Véges testek

Példa folyt.

·	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	0	x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	0	x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	0	2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	0	2x+1	x+2	x+1	2	2x	2x+2	x	1
2x+2	0	2x+2	x+1	2x+1	x	2	x+2	1	2x

Például:

$$(2x + 2)(2x + 1) = 4x^2 + 6x + 2 \stackrel{\mathbb{Z}_3}{=} x^2 + 2 = (x^2 + 1) + 1$$

Feladat: Legyen $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 1)$. Mik lesznek a $z^2 + 1 \in \mathbb{F}_9[z]$ polinom gyökei?