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. tavasz

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).

Emlékeztető

Test nullosztómentes, így F test és $f, g \in F[x]$ esetén:
$\deg(fg) = \deg(f) + \deg(g)$.

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.
Mivel $f \in \mathbb{R}[x]$, ezért $\overline{c}$ is gyöke, hiszen

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

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

Polinomok felbonthatósága

Definíció

$f \in \mathbb{Z}[x]$-et primitív polinomnak nevezzük, ha az együtthatóinak a legnagyobb közös osztója 1.

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.

Bizonyítás

NB. (Lehet, hogy később igen.)

Polinomok felbonthatósága

Megjegyzés

A feltételben f_n és f_0 szerepe felcserélhető.

Megjegyzés

A tétel nem használható test fölötti polinom irreducibilitásának bizonyítására, mert testben nem léteznek prímek, hiszen minden nem-nulla elem egység.

Racionális gyökteszt

Tétel

Legyen $f(x) = f_n x^n + f_{n-1} x^{n-1} + \ldots + f_1 x + f_0 \in \mathbb{Z}[x]$, $f_n \neq 0$ 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

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

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

$p | f_0 q^n$, 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 $q | f_n$.

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

$f \not| g$ 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 prímhatvány, 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:

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

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:

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

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?

A kommunikáció során információt hordozó adatokat viszünk át egy csatornán keresztül az információforrástól, az adótól az információ címzettjéhez, a vevőhöz.

A kommunikáció vázlatos ábrája

Megjegyzés

Az információ átvitele térben és időben történik. Egyes esetekben az egyik, más esetekben a másik dimenzió a domináns (pl. telefonálás; információ rögzítése adathordozóra, majd későbbi visszaolvasása).

Definíció

Az információ új ismeret. Shannon nyomán az általa megszüntetett bizonytalansággal mérjük.

Definíció

Tegyük fel, hogy egy információforrás nagy számú, összesen n üzenetet bocsát ki. Az összes ténylegesen előforduló különböző üzenet legyen $a_1, a_2, \ldots, a_k$.
Ha az a_j üzenet m_j-szer fordul elő, akkor azt mondjuk, hogy a gyakorisága m_j, relatív gyakorisága pedig $p_j = \frac{m_j}{n} > 0$.
A $p_1, p_2, \ldots, p_k$ szám k-ast az üzenetek eloszlásának nevezzük ($\sum_{j=1}^{k} p_j = 1$).
Az a_j üzenet egyedi információtartalma $I_j = -\log_r p_j$, ahol r egy 1-nél nagyobb valós szám, ami az információ egységét határozza meg. Ha $r = 2$, akkor az információ egysége a bit.
Az üzenetforrás által kibocsátott üzenetek átlagos információtartalma, vagyis $H_r(p_1, p_2, \ldots, p_k) = -\sum_{j=1}^{k} p_j \log_r p_j$ a forrás entrópiája. Ez csak az üzenetek eloszlásától függ, a tartalmuktól nem.
Egy k tagú eloszlásnak olyan pozitív valós számokból álló $p_1, p_2, \ldots, p_k$ sorozatot nevezünk, amelyre $\sum_{j=1}^{k} p_j = 1$. Ennek az eloszlásnak az entrópiája $H_r(p_1, p_2, \ldots, p_k) = -\sum_{j=1}^{k} p_j \log_r p_j$.