Diszkrét matematika 2.C szakirány

8. előadás

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

Komputeralgebra Tanszék

2016. ősz

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.

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

Bizonyítás folyt.

Így $m + o = deg(f)$, ahonnan $m = deg(g)$ és $o = deg(h)$. Viszont m és o nem lehet egyszerre pozitív, mert akkor $p^2 | f_0 = g_0 h_0$ teljesülne. Így az egyik polinom konstans, és ha nem lenne egység, akkor f nem lenne primitív.

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 $H_r(p_1, p_2, \ldots, p_k) = -\sum_{j=1}^{k} p_j \log_r p_j$.