Diszkrét matematika 2.C szakirány

6. előadás

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

Komputeralgebra Tanszék

2016. ősz

Bővített euklideszi algoritmus

Definíció

Azt mondjuk, hogy $f, g \in R[x]$ polinomok esetén f osztója g-nek (g többszöröse f-nek), ha létezik $h \in R[x]$, amire $g = f \cdot h$.

Definíció

Az $f, g \in R[x]$ polinomok kitüntetett közös osztója (legnagyobb közös osztója) az a $d \in R[x]$ polinom, amelyre $d|f$, $d|g$, és tetszőleges $c \in R[x]$ esetén $(c|f \wedge c|g) \Rightarrow c|d$.

Test fölötti polinomgyűrűben tetszőleges nem-nulla polinommal tudunk maradékosan osztani, ezért működik a bővített euklideszi-algoritmus. Ez $f, g \in R[x]$ esetén (R test) meghatározza f és g kitüntetett közös osztóját, a $d \in R[x]$ polinomot, továbbá $u, v \in R[x]$ polinomokat, amelyekre $d = u \cdot f + v \cdot g$.

Bővített euklideszi algoritmus

Algoritmus

Legyen R test, $f, g \in R[x]$. Ha $g = 0$, akkor $(f, g) = f = 1 \cdot f + 0 \cdot g$, különben végezzük el a következő maradékos osztásokat:

$$
\begin{aligned}
f &= q_1 g + r_1;\\
g &= q_2 r_1 + r_2;\\
r_1 &= q_3 r_2 + r_3;\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n;\\
r_{n-1} &= q_{n+1} r_n.
\end{aligned}
$$

Ekkor $d = r_n$ jó lesz kitüntetett közös osztónak.
Az $u_{-1} = 1,\ u_0 = 0,\ v_{-1} = 0,\ v_0 = 1$ kezdőértékekkel, továbbá az $u_k = u_{k-2} - q_k \cdot u_{k-1}$ és $v_k = v_{k-2} - q_k \cdot v_{k-1}$ rekurziókkal megkapható $u = u_n$ és $v = v_n$ polinomok olyanok, amelyekre teljesül $d = u \cdot f + v \cdot g$.

Bővített euklideszi algoritmus

Bizonyítás

A maradékok foka természetes számok szigorúan monoton csökkenő sorozata, ezért az eljárás véges sok lépésben véget ér.
Indukcióval belátjuk, hogy $r_{-1} = f$ és $r_0 = g$ jelöléssel $r_k = u_k \cdot f + v_k \cdot g$ teljesül minden $-1 \leq k \leq n$ esetén:
$k = -1$-re $f = 1 \cdot f + 0 \cdot g$, $k = 0$-ra $g = 0 \cdot f + 1 \cdot g$.
Mivel $r_{k+1} = r_{k-1} - q_{k+1} \cdot r_k$, így az indukciós feltevést használva:
$r_{k+1} = u_{k-1} \cdot f + v_{k-1} \cdot g - q_{k+1} \cdot (u_k \cdot f + v_k \cdot g) =$
$= (u_{k-1} - q_{k+1} \cdot u_k) \cdot f + (v_{k-1} - q_{k+1} \cdot v_k) \cdot g = u_{k+1} \cdot f + v_{k+1} \cdot g$.
Tehát $r_n = u_n \cdot f + v_n \cdot g$, és így f és g közös osztói r_n-nek is osztói.
Kell még, hogy r_n osztója f-nek és g-nek.
Indukcióval belátjuk, hogy $r_n | r_{n-k}$ teljesül minden $0 \leq k \leq n+1$ esetén:
$k = 0$-ra $r_n | r_n$ nyilvánvaló, $k = 1$-re $r_{n-1} = q_{n+1} r_n$ miatt $r_n | r_{n-1}$.
$r_{n-(k+1)} = q_{n-(k-1)} r_{n-k} + r_{n-(k-1)}$ miatt az indukciós feltevést használva kapjuk az állítást, és így $k = n$, illetve $k = n+1$ helyettesítéssel $r_n | r_0 = g$, illetve $r_n | r_{-1} = f$.

Polinomok algebrai deriváltja

Definíció

Legyen R gyűrű. Az
$f(x) = f_n x^n + f_{n-1} x^{n-1} + \ldots + f_2 x^2 + f_1 x + f_0 \in R[x]$ $(f_n \neq 0)$ polinom
algebrai deriváltja az
$f'(x) = n f_n x^{n-1} + (n-1) f_{n-1} x^{n-2} + \ldots + 2 f_2 x + f_1 \in R[x]$ polinom.

Megjegyzés

Itt $k f_k = \underbrace{f_k + f_k + \ldots + f_k}_{k \text{ db}}$.

Állítás

Legyen R gyűrű, $a, b \in R$ és $n \in \mathbb{N}^+$. Ekkor $(na)b = n(ab) = a(nb)$.

Bizonyítás

$$(\underbrace{a + a + \ldots + a}_{n \text{ db}})b = (\underbrace{ab + ab + \ldots + ab}_{n \text{ db}}) = a(\underbrace{b + b + \ldots + b}_{n \text{ db}})$$

Polinomok algebrai deriváltja

Állítás

Ha R egységelemes integritási tartomány, akkor az $f \mapsto f'$ algebrai deriválás rendelkezik a következő tulajdonságokkal:

1. konstans polinom deriváltja a nullpolinom;
2. az x polinom deriváltja az egységelem;
3. $(f+g)' = f' + g'$, ha $f, g \in R[x]$ (additivitás);
4. $(fg)' = f'g + fg'$, ha $f, g \in R[x]$ (szorzat differenciálási szabálya).

Megjegyzés

Megfordítva, ha egy R egységelemes integritási tartomány esetén egy $f \mapsto f'$, $R[x]$-et önmagába képező leképzés rendelkezik az előző 4 tulajdonsággal, akkor az az algebrai deriválás.

Polinomok algebrai deriváltja

Állítás

Ha R egységelemes integritási tartomány, $c \in R$ és $n \in \mathbb{N}^+$, akkor $((x-c)^n)' = n(x-c)^{n-1}$.

Bizonyítás

n szerinti TI:
$n = 1$ esetén $(x-c)' = 1 = 1 \cdot (x-c)^0$.
Tfh. $n = k$-ra teljesül az állítás, vagyis $((x-c)^k)' = k(x-c)^{k-1}$.
Ekkor

$$((x-c)^{k+1})' = ((x-c)^k(x-c))' = ((x-c)^k)'(x-c) + (x-c)^k(x-c)' =$$
$$= k(x-c)^{k-1}(x-c) + (x-c)^k \cdot 1 = (x-c)^k(k+1).$$

Ezzel az állítást beláttuk.

Állítás (NB)

Ha R integritási tartomány, $char(R) = p$, és $0 \neq r \in R$, akkor $n \cdot r = 0 \iff p|n$.

Polinomok algebrai deriváltja

Definíció

Legyen R egységelemes integritási tartomány, $0 \neq f \in R[x]$ és $n \in \mathbb{N}^+$.
Azt mondjuk, hogy $c \in R$ az f egy n-szeres gyöke, ha $(x-c)^n | f$, de $(x-c)^{n+1} \not| f$.

Megjegyzés

A definíció azzal ekvivalens, hogy $f(x) = (x-c)^n g(x)$, ahol c nem gyöke g-nek. (Miért?)

Tétel

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $n \in \mathbb{N}^+$ és $c \in R$ az f egy n-szeres gyöke. Ekkor c az f'-nek legalább $(n-1)$-szeres gyöke, és ha $char(R) \not| n$, akkor pontosan $(n-1)$-szeres gyöke.

Polinomok algebrai deriváltja

Bizonyítás

Ha $f(x) = (x-c)^n g(x)$, ahol c nem gyöke g-nek, akkor
$f'(x) = ((x-c)^n)' g(x) + (x-c)^n g'(x) =$
$= n(x-c)^{n-1} g(x) + (x-c)^n g'(x) = (x-c)^{n-1}(ng(x) + (x-c)g'(x))$.
Tehát c tényleg legalább $(n-1)$-szeres gyöke f'-nek, és akkor lesz $(n-1)$-szeres gyöke, ha c nem gyöke $ng(x) + (x-c)g'(x)$-nek, vagyis $0 \neq ng(c) + (c-c)g'(c) = ng(c) + 0 \cdot g'(c) = ng(c)$. Ez pedig teljesül, ha $char(R) \nmid n$.

Példa

Legyen $f(x) = x^4 - x \in \mathbb{Z}_3[x]$. Ekkor 1 3-szoros gyöke f-nek, mert

$$f(x) = x(x^3 - 1) \overset{\mathbb{Z}_3}{=} x(x^3 - 3x^2 + 3x - 1) = x(x-1)^3.$$
$$f'(x) = 4x^3 - 1 \overset{\mathbb{Z}_3}{=} x^3 - 3x^2 + 3x - 1 = (x-1)^3,$$

tehát 1 3-szoros gyöke f'-nek is.

Lagrange-interpoláció

Tétel

Legyen R test, $c_0, c_1, \dots, c_n \in R$ különbözőek, továbbá $d_0, d_1, \dots, d_n \in R$ tetszőlegesek. Ekkor létezik egy olyan legfeljebb n-ed fokú polinom, amelyre $f(c_j) = d_j$, ha $j = 0, 1, \dots, n$.

Bizonyítás

Legyen

$$l_j(x) = \frac{\prod_{i \neq j}(x - c_i)}{\prod_{i \neq j}(c_j - c_i)},$$

a j-edik Lagrange-interpolációs alappolinom, és legyen

$$f(x) = \sum_{j=0}^{n} d_j l_j(x).$$

$l_j(c_i) = 0$, ha $i \neq j$, és $l_j(c_j) = 1$-ből következik az állítás.

Lagrange-interpoláció

Példa

Adjunk meg olyan $f \in \mathbb{R}[x]$ polinomot, amelyre $f(0) = 3$, $f(1) = 3$, $f(4) = 7$ és $f(-1) = 0$!

A feladat szövege alapján $c_0 = 0$, $c_1 = 1$, $c_2 = 4$, $c_3 = -1$, $d_0 = 3$, $d_1 = 3$, $d_2 = 7$ és $d_3 = 0$ értékekkel alkalmazzuk a Lagrange-interpolációt.

$l_0(x) = \frac{(x-1)(x-4)(x+1)}{(0-1)(0-4)(0+1)} = \frac{1}{4}x^3 - x^2 - \frac{1}{4}x + 1$

$l_1(x) = \frac{(x-0)(x-4)(x+1)}{(1-0)(1-4)(1+1)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 + \frac{2}{3}x$

$l_2(x) = \frac{(x-0)(x-1)(x+1)}{(4-0)(4-1)(4+1)} = \frac{1}{60}x^3 - \frac{1}{60}x$

$l_3(x) = \frac{(x-0)(x-1)(x-4)}{(-1-0)(-1-1)(-1-4)} = -\frac{1}{10}x^3 + \frac{1}{2}x^2 - \frac{2}{5}x$

$f(x) = 3l_0(x) + 3l_1(x) + 7l_2(x) + 0l_3(x) = \frac{22}{60}x^3 - \frac{3}{2}x^2 + \frac{68}{60}x + 3$

	$\frac{22}{60}$	$-\frac{3}{2}$	$\frac{68}{60}$	3	
1	$\times$	$\frac{22}{60}$	$-\frac{68}{60}$	0	3
4	$\times$	$\frac{22}{60}$	$-\frac{2}{60}$	1	7
-1	$\times$	$\frac{22}{60}$	$-\frac{112}{60}$	3	0

Lagrange-interpoláció

Alkalmazás

A Lagrange-interpoláció használható titokmegosztásra a következő módon:
legyenek $1 \leq m < n$ egészek, továbbá $s \in \mathbb{N}$ a titok, amit n ember között akarunk szétosztani úgy, hogy bármely m részből a titok rekonstruálható legyen, de kevesebből nem. Válasszunk a titok maximális lehetséges értékénél és n-nél is nagyobb p prímet, továbbá $a_1, a_2, \ldots, a_{m-1} \in \mathbb{Z}_p$ véletlen együtthatókat, majd határozzuk meg az
$f(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_1x + s$ polinomra az $f(i)$ értékeket, és adjuk ezt meg az i. embernek $(i = 1, 2, \ldots, n)$.
Bármely m helyettesítési értékből a Lagrange-interpolációval megkapható a polinom, így annak konstans tagja is, a titok.
Ha m-nél kevesebb helyettesítési értékünk van, akkor nem tudjuk meghatározni a titkot, mert tetszőleges t esetén az $f(0) = t$ értéket hozzávéve a többihez létezik olyan legfeljebb m-ed fokú polinom, aminek a konstans tagja t, és az adott helyeken megfelelő a helyettesítési értéke.

Titokmegosztás

Példa

Legyen $m = 3$, $n = 4$, $s = 5$, $p = 7$, továbbá $a_1 = 3$ és $a_2 = 4$. Ekkor $f(x) = 4x^2 + 3x + 5 \in \mathbb{Z}_7[x]$, a titokrészletek pedig $f(1) = 5$, $f(2) = 6$, $f(3) = 1$ és $f(4) = 4$. Ha rendelkezünk például az $f(1) = 5$, $f(3) = 1$ és $f(4) = 4$ információkkal, akkor $c_0 = 1$, $c_1 = 3$, $c_2 = 4$, $d_0 = 5$, $d_1 = 1$, és $d_2 = 4$ értékekkel alkalmazzuk a Lagrange-interpolációt.

$l_0(x) = \frac{(x-3)(x-4)}{(1-3)(1-4)} = \frac{1}{6}(x^2 - 7x + 12) = \frac{1}{-1}(-6x^2 - 2) = 6x^2 + 2$

$l_1(x) = \frac{(x-1)(x-4)}{(3-1)(3-4)} = -\frac{1}{2}(x^2 - 5x + 4) = -4(x^2 + 2x + 4) = 3x^2 + 6x + 5$

$l_2(x) = \frac{(x-1)(x-3)}{(4-1)(4-3)} = \frac{1}{3}(x^2 - 4x + 3) = 5(x^2 + 3x + 3) = 5x^2 + x + 1$

$f(x) = 5l_0(x) + l_1(x) + 4l_2(x) = 30x^2 + 10 + 3x^2 + 6x + 5 + 20x^2 + 4x + 4 =$
$= 53x^2 + 10x + 19 = 4x^2 + 3x + 5$

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).