

# תרגול 10 - חילוק פולינומים

31 במאי 2021

## 1 חוג הפולינומים

משפט (חילוק פולינומים): יהא  $\mathbb{F}$  שדה.  $\mathbb{F}[x]$  חוג הפולינומים. אזי לכל  $a(x), b(x) \in \mathbb{F}[x]$  כך ש  $b(x) \neq 0$  קיימים  $q(x), r(x)$  כך ש

$$a(x) = q(x)b(x) + r(x)$$

המקיימים  $deg(r) < deg(b)$  או  $r = 0$ . והם יחידים.

סימון  $b|a$  אם קיים  $q$  כך ש  $a = qb$ , כלומר,  $\frac{a}{b} = q$ .

((קיום gcd)): יהא  $\mathbb{F}$  שדה.  $\mathbb{F}[x]$  חוג הפולינומים. אזי לכל  $a(x), b(x) \in \mathbb{F}[x]$  קיים פולינום מתוקן (מתוקן הכוונה שהמקדם של החזקה הגבוהה הוא 1)  $d(x) = \gcd(a, b)$  המקיים:

1.  $d | a, b$

2. אם  $d' | a, b$  אז  $deg(d') \leq deg(d)$ .

3. בנוסף קיימים  $m(x), n(x)$  כך ש

$$d = an + bm$$

משפט: אם  $a(x) = q(x)b(x) + r(x)$ , אז:

$$\gcd(a(x), b(x)) = \gcd(b(x), r(x))$$

וכמובן, כאשר  $r_{k+1}(x) = 0$ , אז  $\gcd(a, b) = r_k$ . הערה: אם  $r_k$  קבוע ( $deg(r_k) = 0$ ), אז  $r_{k+1} = 0$ .

הוכחה: נראה בכיוון אחד שאם  $d|a, b$  אז  $d|r$ . בכיוון שני, אם  $d|b, r$  אז  $d|a$ . בטה"כ נקבל שקבוצת המחלקים המשותפים של  $a, b$  שווה לקבוצת המחלקים המשותפים של  $b, r$ , ולכן הגדול מביניהם (מבחינת דרגה) הוא אותו אחד. כיוון ראשון: נניח  $d|a, b$ , כלומר: ישנם  $m, n$  כך ש-

$$a = dm, b = dn$$

ולכן, מכיון ש-  $a = bq + r$  אז

$$r = a - bq = dm - dnq = d(m - nq)$$

קיבלנו ש- $r$  הוא כפולה של  $d$ , מה שאומר  $d|r$ . כיוון שני: נניח  $d|b, r$ , כלומר, ישנם  $m, n$  כך ש-

$$b = dn, r = dm$$

ולכן:

$$a = qb + r = qdn + dm = d(qn + m)$$

ולכן  $d|a$ .

תרגילים:

1.  $a(x) = x^6 + x^5 + x^4 + x^2 + 1, b(x) = 1 + x + x^3$ . חלק את  $a$  ב  $b$  ומצאו  $\gcd(a, b)$ . והציגו אותו כצ"ל של  $a, b$ . פתרון

$q_1(x) = x^3 + x^2 - 2$	$x^3 + x + 1$
$x^6 + x^5 + x^4 + x^2 + 1$	$x^6 + x^4 + x^3$
	↓
$x^5 - x^3 + x^2 + 1$	$x^5 + x^3 + x^2$
	↓
$-2x^3 + 1$	$-2x^3 - 2x - 2$
	↓
$r_1 = 2x + 3$	

כלומר, קיבלנו כעת:  $a = q_1 \cdot b + r_1$ , או:  $x^6 + x^5 + x^4 + x^2 + 1 = (x^3 + x^2 - 2)(x^3 + x + 1) + (2x + 3)$

$2x + 3$ . כעת, נמשיך ונחשב את החילוק  $\frac{b}{r_1}$ .

$$\begin{array}{r|l}
 q_2(x) = \frac{1}{2}x^2 - \frac{3}{4}x + \frac{13}{8} & \\
 \hline
 x^3 + x + 1 & 2x + 3 \\
 x^3 + \frac{3}{2}x^2 & \\
 \downarrow & \\
 -\frac{3}{2}x^2 + x + 1 & \\
 -\frac{3}{2}x^2 - \frac{9}{4}x & \\
 \downarrow & \\
 \frac{13}{4}x + 1 & \\
 \frac{13}{4}x + \frac{39}{8} & \\
 \downarrow & \\
 r_2(x) = -\frac{31}{8} & 
 \end{array}$$

ולכן  $r_1(x) = 2x + 3 = q_3 \cdot r_2 = \left(-\frac{16}{31}x - \frac{24}{31}\right) \cdot \left(-\frac{31}{8}\right) = 2x + 3$  במילים אחרות: קיבלנו  $r_2(x)$  קבוע, ולכן נוכל לוותר על השלב הבא, ולקבוע:

$$\gcd(a, b) = 1$$

נמצא כעת פולינומים  $m(x), n(x)$  כך ש-

$$1 = m(x)a(x) + n(x)b(x)$$

האלגוריתם נתן לנו:

$$b(x) = q_2(x)r_1(x) + r_2(x)$$

נעביר אגפים:

$$r_2(x) = b(x) - q_2(x)r_1(x)$$

ונציב כעת את  $r_1$  מהשלב האשון:

$$a(x) = q_1(x)b(x) + r_1(x) \iff r_1(x) = a(x) - q_1(x)b(x)$$

נציב ונקבל:

$$r_2(x) = b(x) - q_2(x)(a(x) - q_1(x)b(x)) = \underbrace{-q_2(x)a(x)} + \underbrace{(1 + q_1(x)q_2(x))b(x)}$$

ננרמל את  $r_2$  ונקבל:

$$1 = -\frac{8}{31}r_2(x) = \underbrace{\frac{8}{31}q_2(x)a(x)}_{m(x)} + \underbrace{-\frac{8}{31}(1 + q_1(x)q_2(x))b(x)}_{n(x)}$$

$$.a(x) = x^3 + 4x^2 + 2x - 3, b(x) = x^2 + 2x - 3 \quad 2.$$

פתרון:

$q_1 = x + 2$	
$x^3 + 4x^2 + 2x - 3$	$x^2 + 2x - 3$
$x^3 + 2x^2 - 3x$	
↓	
$2x^2 + 5x - 3$	
$2x^2 + 4x - 6$	
↓	
$r_1 = x + 3$	

קיבלנו:  $a = (x + 2)(x^2 + 2x - 3) + x + 3$  שלב שני:

$q_2 = x - 1$	
$x^2 + 2x - 3$	$x + 3$
$x^2 + 3x$	
↓	
$-x - 3$	
$-x - 3$	
↓	
$r_2 = 0$	

קיבלנו  $r_2 = 0$  ולכן  $\text{gcd}(a, b) = r_1 = x + 3$  כעת:

$$a = q_1 b + r_1$$

ולכן:

$$r_1 = a - q_1 b$$

$$\text{כלומר, } m(x) = 1, n(x) = -q_1$$