

# שעור 10

## פולינומים

### 10.1 חילוק פולינומים, פולינום המינימלי ופולינומים שמתאפסים ע"י מטריצה

#### משפט 10.1

הפולינום המינימלי הוא יחיד.

**הוכחה:** נניח שיש שני פולינומים  $f_1(x)$  ו- $f_2(x)$  מאותו סדר, כלומר

$$f_1(x) = \alpha_0 + \alpha_1 x + \dots + \alpha_{k-1} x^{k-1} + x^k,$$

$$f_2(x) = \beta_0 + \beta_1 x + \dots + \beta_{k-1} x^{k-1} + x^k.$$

כך ש  $f_1(A) = 0$  ו- $f_2(A) = 0$ , אז

$$(f_1 - f_2)(A) = 0.$$

פולינום מסדר קטן מ- $k$ . סתירה. ■

#### משפט 10.2 משפט חילוק של פולינומים

יהיו  $f(x), g(x)$  פולינומים כך ש- $\deg g \leq \deg f$ . אז קיימים פולינומים  $q(x), r(x)$  יחידים כך ש

$$f(x) = q(x) \cdot g(x) + r(x)$$

כאשר

$$\deg r(x) < \deg g(x), \quad \deg g(x) \leq \deg f(x).$$

#### משפט 10.3 פולינום שמתאפס ע"י $A$ מחלק את הפולינום המינימלי

תהי  $A \in \mathbb{F}^{n \times n}$  מטריצה ריבועית ויהי  $f(x)$  פולינום. אם  $f(A) = 0$  אז

$$m_A(x) \mid f(x).$$

**הוכחה:** נחלק את  $f(x)$  ב- $m_A(x)$ . לפי משפט חילוק פולינומים,

$$f(x) = m_A(x) \cdot q(x) + r(x)$$

כאשר  $\deg r(x) < \deg m_A(x)$ . אז

$$f(A) = q(A)m_A(A) + r(A).$$

$f(A) = 0$  ו- $m_A(A) = 0$  לכן  $r(A) = 0$ .

ז"א או  $r(x)$  הוא הפולינום האפס או הוא לא פולינום האפס אבל  $r(x)$  מתאפס ע"י  $A$ .  
 $m_A(x)$  הוא הפולינום המינימלי ו  $\deg r(x) < \deg m_A(x)$ , כלומר  $m_A(x)$  הוא הפולינום מדרגה הכי נמוכה המתאפס ע"י  $A$ .

לכן  $r(A) = 0$  אם  $r(x) = 0$ , כלומר  $r(x)$  פולינום האפס.  
 כלומר קיבלנו ש-  $f(x) = q(x) \cdot m_A(x)$  ולכן  $f(x) \mid m_A(x)$ .

### מסקנה 10.1 פולינום המינימלי מחלק את הפולינום האופייני

תהי  $A \in \mathbb{F}^{n \times n}$  מטריצה ריבועית. אם  $p_A(x)$  הפולינום האופייני ו-  $m_A(x)$  הפולינום המינימלי של  $A$ , אז

$$m_A(x) \mid p_A(x).$$

**הוכחה:** לפי משפט קיילי המילטון,  $p_A(A) = 0$ . הפולינום המינימלי מחלק כל פולינום המתאפס ע"י  $A$ , לכן  $m_A(x) \mid p_A(x)$ .

### משפט 10.4 $p_A(x)$ מחלק כל פולינום המתאפס ע"י $A$ בחזקת הסדר של $A$ .

תהי  $A \in \mathbb{F}^{n \times n}$  מטריצה ריבועית. יהי  $p_A(x)$  הפולינום האופייני של  $A$ . אם  $A$  מאפסת את הפולינום  $f(x)$ , כלומר אם  $f(A) = 0$ , אז

$$p_A(x) \mid f^n(x).$$

**הוכחה:**  $\deg p_A(x) = n$ .  $f(A) = 0$  אז  $f(x)$  אינו פולינום קבוע, ז"א  $\deg f(x) \geq 1$ , ולכן  $\deg p_A(x) \leq \deg f^n(x)$ . נחלק  $f^n(x)$  ב-  $p_A(x)$  ע"י האלגוריתם איוקלידי:

$$f^n(x) = q(x)p_A(x) + r(x), \quad (*)1$$

$$\deg r(x) < \deg p_A(x) \leq \deg f^n(x)$$

$$m_A(x) \mid p_A(x) \text{ אז } p_A(x) = q_1(x)m_A(x) \text{ נציב זה ב- } (*)1 \text{ ונקבל}$$

$$f^n(x) = q_1(x)q(x)m_A(x) + r(x). \quad (*)2$$

$f(A) = 0$  לכן  $f^n(A) = 0$  לכן  $f^n(x) \mid m_A(x)$ . נניח ש-  $r(x) \neq 0$  ב-  $(*)2$ . אז  $f^n(x) \nmid m_A(x)$ . סתירה.

### משפט 10.5 גורם אי-פריק של הפולינום האופייני מחלק כל פולינום המתאפס ע"י $A$ .

תהי  $A \in \mathbb{F}^{n \times n}$  מטריצה ריבועית. יהי  $p_A(x)$  הפולינום האופייני של  $A$ . אם  $(x - \lambda_0)$  גורם אי פריק של  $p_A(x)$  ו-  $f(x)$  פולינום המתאפס ע"י  $A$ , כלומר אם  $f(A) = 0$ , אז

$$(x - \lambda_0) \mid f(x).$$

**הוכחה:**

אם  $(x - \lambda_0)$  גורם אי-פריק של  $p_A(x)$ , אז  $\lambda_0$  ערך עצמי של  $A$ . נחלק  $f(x)$  ב-  $(x - \lambda_0)$ . כלומר לפי משפט חילוק פולינומים קיימים פולינומים יחידים  $q(x), r(x)$  כך ש-

$$f(x) = q(x)(x - \lambda_0) + r(x)$$

כאשר  $\deg r(x) < \deg (x - \lambda_0) \leq \deg f(x)$ .  
 $\deg r(x) = 0$  אז  $\deg (x - \lambda_0) = 1$ .  
 ז"א  $r(x)$  פולינום קבוע:  $r(x) = c \in \mathbb{F}$  כאשר  $c$  סקלר.  
 יהי  $v$  וקטור עצמי השייך ל- $\lambda_0$  אז

$$0 = f(A)v = q(A)(A - \lambda_0 I)v + cv$$

$v$  הוא הוקטור עצמי השייך ל- $\lambda_0$ , אז  
 $(A - \lambda_0)v = Av - \lambda_0 v = \lambda_0 v - \lambda_0 v = 0$ .  
 לכן  $c = 0$ , ואז נקבל

$$f(x) = q(x)(x - \lambda_0),$$

ז"א  $(x - \lambda_0) \mid f(x)$ .

## 10.2 מחלק משותף

### הגדרה 10.1 מחלק משותף

יהיו  $p_1(x), \dots, p_k(x) \in \mathbb{F}[x]$  פולינומים מעל שדה  $\mathbb{F}$ . פולינום  $h(x) \in \mathbb{F}[x]$  נקרא **מחלק משותף של**  $p_1(x), \dots, p_k(x)$  אם לכל  $1 \leq i \leq k$  מחלק את  $p_i(x)$ .

### הגדרה 10.2 מחלק משותף מקסימלי

יהיו  $p_1(x), \dots, p_k(x) \in \mathbb{F}[x]$  פולינומים שונים מאפס מעל שדה  $\mathbb{F}$ . פולינום מתוקן  $h(x) \in \mathbb{F}[x]$  נקרא **מחלק משותף מקסימלי של**  $p_1(x), \dots, p_k(x)$  אם:

(1)  $h(x)$  מחלק משותף של  $p_1(x), \dots, p_k(x)$ .

(2) אם  $q(x)$  הוא מחלק משותף של  $p_1(x), \dots, p_k(x)$  אז  $q(x)$  מחלק גם את  $h(x)$ .

מחלק משותף מקסימלי מסומן ב-  $\gcd(p_1, p_2, \dots, p_k)$  (greatest common divisor).

### משפט 10.6

יהיו  $p_1(x), \dots, p_k(x) \in \mathbb{F}[x]$  פולינומים שונים מאפס מעל שדה  $\mathbb{F}$ . נגדיר

$$I = \{q_1 p_1 + q_2 p_2 + \dots + q_k p_k \mid q_1, q_2, \dots, q_k \in \mathbb{F}[x]\}$$

כלומר,  $I$  הוא אוסף כל "הצירופים הליניאריים" של  $p_1(x), \dots, p_k(x)$  כאשר ה"מקדמים" הם הפולינומים  $q_1(x), q_2(x), \dots, q_k(x)$ . מתקיים:

(1)  $p_1(x), \dots, p_k(x) \in I$

(2) אם  $L(x) \in I$  ואם  $q(x) \in \mathbb{F}[x]$  אז  $q(x)L(x) \in I$

(3)  $I$  תת-מרחב ליניארי של  $\mathbb{F}[x]$

## משפט 10.7

יהיו  $p_1(x), \dots, p_k(x) \in \mathbb{F}[x]$  פולינומים שזים מאפס מעל שדה  $\mathbb{F}$ . נגדיר

$$I = \{q_1(x)p_1(x) + q_2(x)p_2(x) + \dots + q_k(x)p_k(x) \mid q_1(x), q_2(x), \dots, q_k(x) \in \mathbb{F}[x]\}$$

נניח גם שלפחות אחד מהפולינומים  $p_1(x), \dots, p_k(x)$  אינו פולינום האפס.

(1) קיים פולינום מתוקן  $h(x) \in I$  כך שזום פולינום שמעלתו קטנה ממעלתו של  $h(x)$  סרט לפולינום האפס אינו שייך ל- $I$ .

(2)  $h(x)$  הוא מחלק משותף של  $p_1(x), p_2(x), \dots, p_k(x)$ .

(3) אם  $k(x) \in \mathbb{F}[x]$  הוא מחלק משותף של  $p_1(x), p_2(x), \dots, p_k(x)$  אז  $k(x)$  מחלק גם את  $h(x)$ .

הוכחה:

(1) לפחות אחד מהפולינומים  $p_1(x), p_2(x), \dots, p_k(x)$  אינו פולינום האפס, נסיק מחלק (1) של טענה 10.6 שיש ב- $I$  לפחות פולינום אחד שאינו אפס כלומר פולינום שמעלתו אי-שלילית. לכל קבוצה לא ריקה של מספרים שלמים אי-שליליים קיים מינימום, נובע שקיים פולינום  $\hat{h}(x) \in I$  ממעלה מינימלית. כלומר, שום פולינום שמעלתו קטנה ממעלתו של  $\hat{h}(x)$  פרט לפולינום האפס אינו שייך ל- $I$ . אם נסמן ב- $a \neq 0 \in \mathbb{F}$  את המקדם העליון של  $\hat{h}(x)$  אז הפולינום  $h(x) = a^{-1}\hat{h}(x)$  הוא פולינום מתוקן. ממשפט 10.6 סעיף (3) נובע ש- $h(x) \in I$ . מעלתו של  $h(x)$  שווה למעלתו של  $\hat{h}(x)$ . נובע שזום פולינום שמעלתו קטנה ממעלתו של  $h(x)$  פרט לפולינום האפס, אינו שייך ל- $I$ .

(2) יהי  $L(x) \in I$ . נוכיח שקיים  $q(x) \in \mathbb{F}[x]$  כך ש- $L(x) = q(x)h(x)$ . מכיוון ש- $h(x)$  אינו פולינום האפס ניתן לחלק את  $L(x)$  ב- $h(x)$  עם שארית:

$$L(x) = q(x)h(x) + r(x)$$

כאשר  $\deg(r) < \deg(h)$ . מכיוון ש- $h(x), L(x) \in I$  אזי מסעיפים (2) ו-(3) של משפט 10.6  $r(x) = L(x) - h(x)q(x) \in I$ . מכיוון ש- $\deg(r) < \deg(h)$  נסיק מתכונת מינימליות של  $h(x)$  ש- $r(x) = 0$ .

לכן  $L(x) = q(x)h(x)$  ולכן  $h(x)$  מחלק  $L(x)$ .

(3) יהיו  $g_1(x), g_2(x), \dots, g_k(x) \in \mathbb{F}[x]$  פולינומים המקיימים

$$p_1(x) = g_1(x)k(x), \quad p_2(x) = g_2(x)k(x), \quad \dots \quad p_k(x) = g_k(x)k(x).$$

מכיוון ש- $h(x) \in I$  נובע שקיימים  $q_1(x), q_2(x), \dots, q_k(x) \in \mathbb{F}[x]$  שעבורם

$$h(x) = q_1p_1(x) + \dots + q_kp_k(x).$$

לכן

$$h(x) = q_1(x)g_1(x)k(x) + \dots + q_k(x)g_k(x)k(x) = \left( q_1(x)g_1(x) + \dots + q_k(x)g_k(x) \right) k(x)$$

כלומר  $k(x)$  מחלק את  $h(x)$ .

### משפט 10.8

יהיו  $p_1(x), \dots, p_k(x) \in \mathbb{F}[x]$  פולינומים שונים מאפס מעל שדה  $\mathbb{F}$ . נניח גם שלפחות אחד מהפולינומים  $p_1(x), \dots, p_k(x)$  אינו פולינום האפס.

(1) קיים מחלק משותף מקסימלי יחיד  $h(x) \in \mathbb{F}[x]$  ל-  $p_1(x), \dots, p_k(x)$ .

(2) קיימים  $q_1(x), \dots, q_k(x) \in \mathbb{F}[x]$  שעבורם  $h = q_1 p_1 + q_2 p_2 + \dots + q_k p_k$ .

**הוכחה:** קיומו של מחלק משותף מקסימלי נובע משפט ?? והגדרה 10.2. במהלך ההוכחה של חלק (3) של טענה ?? הוכחנו גם את קיומו של  $q_1(x), \dots, q_k(x) \in \mathbb{F}[x]$  כנדרש.

נותרנו עם הוכחת היחידות.

אם  $h(x), h'(x)$  הם מחלקים משותפים מקסימליים של  $p_1(x), \dots, p_k(x)$  אז מתכונת (2) בהגדרה 10.2 נובע שהם מחלקים זה את זה. שני פולינומים מתוקנים שמחלקים זה את זה הם שווים. ■

### הגדרה 10.3 פולינומים זרים

יהיו  $p_1(x), p_2(x)$  פולינומים מעל שדה  $\mathbb{F}$ .

אומרים כי  $p_1$  ו-  $p_2$  זרים אם אין להם מחלקים משותפים פרט לפולינומי הקבועים.

במילים אחרות,  $p_1$  ו-  $p_2$  זרים אם  $\gcd(p_1, p_2) = 1$ .

### משפט 10.9 פולינומים זרים

יהיו  $p_1(x), p_2(x) \in \mathbb{F}[x]$  פולינומים שאינם אפס.

$p_1$  ו-  $p_2$  זרים אם ורק אם קיימים פולינומים  $q_1(x), q_2(x)$  שעבורם  $q_1(x)p_1(x) + q_2(x)p_2(x) = 1$ .

**הוכחה:**

כיוון אם

אם  $\gcd(p_1, p_2) = 1$  אז ממשפט 10.8 נובע שקיימים  $q_1(x), q_2(x) \in \mathbb{F}[x]$  שעבורם  $q_1(x)p_1(x) + q_2(x)p_2(x) = 1$ .

כיוון רק אם

נניח שקיימים  $q_1(x), q_2(x) \in \mathbb{F}[x]$  שעבורם  $q_1(x)p_1(x) + q_2(x)p_2(x) = 1$ . יהי  $k(x)$  מחלק משותף של  $p_1$  ו-  $p_2$ . עלינו להוכיח ש-  $\deg(k) = 0$ . לשם כך, די להוכיח ש-  $k(x)$  מחלק את 1. ואמנם קיימים פולינומים  $g_1, g_2 \in \mathbb{F}[x]$  כך ש-

$$p_1(x) = g_1(x)k(x), \quad p_2(x) = g_2(x)k(x).$$

לכן,

$$1 = q_1(x)g_1(x)k(x) + q_2(x)g_2(x)k(x) = \left( q_1(x)g_1(x) + q_2(x)g_2(x) \right) k(x).$$

בפרט,  $k(x)$  מחלק את 1.

## 10.3 כפולה משותפת

### הגדרה 10.4 כפולה משותפת

יהיו  $p_1(x), \dots, p_k(x) \in \mathbb{F}[x]$  פולינומים שונים מאפס מעל שדה  $\mathbb{F}$ . פולינום  $q(x) \in \mathbb{F}[x]$  נקרא **כפולה משותפת של**  $p_1(x), \dots, p_k(x)$  אם לכל  $1 \leq i \leq k$  מחלק את  $q(x)$ .

### הגדרה 10.5 כפולה משותפת מינימלית

יהיו  $p_1(x), \dots, p_k(x) \in \mathbb{F}[x]$  פולינומים שונים מאפס. פולינום מתוקן  $q(x) \in \mathbb{F}[x]$  נקרא **כפולה משותפת מינימלית של**  $p_1(x), \dots, p_k(x)$  אם:

(1)  $q(x)$  הוא כפולה משותפת של  $p_1(x), \dots, p_k(x)$ .

(2) שום פולינום שמעלתו קטנה ממעלתו של  $q(x)$  פרט לפולינום האפס, אינו כפולה משותפת של  $p_1(x), \dots, p_k(x)$ .