

## 1 פולינומים (על קצה המזלג)

**הגדרה 1.** פולינום הוא פונקציה מהצורה  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , כאשר  $a_0, a_1, \dots, a_n \in \mathbb{F}$ .

**הערה 1.** ניתן להגדיר לכל  $\alpha \in \mathbb{F}$ ,  $f(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0$ .  
נגדיר חיבור וכפל פולינומים באופן הבא: עבור  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$   
 $g(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$

1.

$$f + g := \sum_{j=0}^{\max\{m,n\}} (a_j + b_j) x^j$$

(כאשר לכל  $i > n$ ,  $a_i = 0$  ולכל  $i > m$ ,  $b_i = 0$ ). במילים אחרות - חיבור לפי החזקות.

2.

$$fg = f \cdot g := a_0 b_0 + (a_1 b_0 + a_0 b_1) x + (a_2 b_0 + a_1 b_1 + a_0 b_2) x^2 + \dots$$

עם ההגדרות הללו מתקיים  $(fg)(\alpha) = f(\alpha)g(\alpha)$  ו- $(f+g)(\alpha) = f(\alpha) + g(\alpha)$ .  
נתחיל ממשפט, המוכר מהלימודים כבר בתיכון. אנו יודעים כי אם יש לנו שני פולינומים, אפשר לחלק אחד בשני, ולקבל מנה ושארית. המשפט הבא מנסח את הטענה באופן כללי:

**משפט 1.** יהיו  $f(x), g(x) \in \mathbb{F}[x]$ , פולינומים,  $\deg(f) \geq 1$ ,  $\deg(g) \geq 1$  (כזכור,  $\deg =$  הדרגה של הפולינום). אזי קיימים פולינומים  $q(x)$  (המנה) ו- $r(x)$  (השארית) שעבורם:

$$f(x) = q(x)g(x) + r(x) \quad 1.$$

$$\deg(r) < \deg(g) \text{ או } r(x) = 0 \quad 2.$$

לא נוביח את המשפט בקורס זה.

**הערה 2.** נעיר מספר הערות על המשפט.

1. בתנאי השני, הסיבה למקרה  $r(x) = 0$  היא ש- $\deg(0)$  אינו מוגדר.

2. אם  $\deg(f) < \deg(g)$ , אז החלוקה הינה  $f(x) = 0 \cdot g(x) + f(x)$ .

3. השוויון בתנאי הראשון הוא שוויון פולינומים (ולא רק של קבוצות הערכים שלהם). בדוגמה הבאה נראה דוגמה לשני פולינומים שונים, המקבלים אותה קבוצת ערכים.

**דוגמה 1.** נדגים שני פולינומים שונים עם אותן קבוצות ערכים, זאת אומרת  $f \neq g$ , אבל

$$f(x) = g(x) \text{ מתקיים } x \in \mathbb{F}$$

עבור השדה  $\mathbb{F} = \mathbb{Z}_2$ , הפולינומים  $f(x) = x^2 - 1$  ו- $g(x) = x$  מקיימים את הדרישות האלו. זה נכון, מפני שמתקיים

$$0^2 = 0, \quad 1^2 = 1$$

