

הגדרה:

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:

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 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ ו- $g(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$

1. $(\sum_{j=0}^{\max\{m,n\}} (a_j + b_j) x^j)$ כאשר לכל $a_i = 0, i > n$ ולכל $b_i = 0, i > m$.
במילים אחרות - חיבור לפי החזקות.

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

עם ההגדרות הללו מתקיים $(f+g)(\alpha) = f(\alpha) + g(\alpha)$ ו- $(fg)(\alpha) = f(\alpha)g(\alpha)$.