משפט החלוקה של פולינומים

בועז צבאן

4 בנובמבר 2012

בקובץ זה נוכיח את משפט החלוקה של פולינומים.

משפט. יהיו $f(x), g(x) \in \mathbb{F}[x]$ פולינומים, כך שמעלת $g(x)$ היא לפחות 1. אזי: יש פולינומים $q(x), r(x) \in \mathbb{F}[x]$ כך שמתקיים

1. $f(x) = q(x) \cdot g(x) + r(x)$.
2. מעלת $r(x)$ קטנה ממעלת $g(x)$.

הוכחה: יהיו k מעלת הפולינום $f(x)$ ו m מעלת הפולינום $g(x)$. נתון ש $1 \leq m$. הוכחת המשפט היא באינדוקציה על k.

בסיס האינדוקציה: $k < m$. כיון ש

$$f(x) = 0 \cdot g(x) + f(x),$$

נוכל לקחת $q(x) = 0, r(x) = f(x)$ ומתקיימות שתי הדרישות.

שלב האינדוקציה ($m \leq k$): נניח שהמשפט נכון עבור פולינומים ממעלה קטנה מ k, ונוכיח עבור פולינומים ממעלה k.

נכתוב את הפולינומים $f(x), g(x)$ במפורש:

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + a_k x^k$$
$$g(x) = b_0 + b_1 x + \cdots + b_{m-1}x^{m-1} + b_m x^m$$

כאשר a_k, b_m שונים מאפס. נגדיר פולינום מאותה מעלה ועם אותו מקדם מוביל כמו $f(x)$:

$$h(x) = \frac{a_k}{b_m}x^{k-m}g(x) = \frac{a_k}{b_m}x^{k-m}((b_0 + b_1 x + \cdots + b_{m-1}x^{m-1}) + b_m x^m) = \frac{a_k}{b_m}x^{k-m}(b_0 + b_1 x + \cdots + b_{m-1}x^{m-1}) + a_k x^k.$$

אז מעלת $f(x) - h(x)$ קטנה מ k. מהנחת האינדוקציה, יש פולינומים $q_0(x), r(x)$ כך ש $f(x) - h(x) = q_0(x) \cdot g(x) + r(x)$ ומעלת $r(x)$ קטנה ממעלת $g(x)$. נעביר את $h(x)$ אגף, ונקבל

$$f(x) = q_0(x) \cdot g(x) + h(x) + r(x) = q_0(x) \cdot g(x) + \frac{a_k}{b_m}x^{k-m}g(x) + r(x) = \underbrace{\left(q_0(x) + \frac{a_k}{b_m}x^{k-m}\right)}_{q(x) \in \mathbb{F}[x]} \cdot g(x) + r(x).$$

כדרוש. ∎