

תרגיל מספר 10 מבנים אלגבריים

1. יהיו $a(x), b(x) \in \mathbb{F}[x]$ שני פולינומים. נחלק את $a(x)$ ב $b(x)$ ע"י אלגוריתם לחילוק פולינומים ונקבל $q(x), r(x)$ כך ש

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

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

2. יהיו $a(x), b(x), c(x) \in \mathbb{F}[x]$ שלושה פולינומים הוכיחו כי אם $\gcd(a(x), c(x)) = \gcd(b(x), c(x)) = 1$ אזי

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

3. תרגיל: הוכיחו כי אם $p(x) \in \mathbb{F}[x]$ פולינום (מדרגה גדולה ממש מאפס) אי פריק אזי הוא ראשוני. [היעזרו בתרגיל הקודם]

4.

(א) נגדיר: $a(x) = 1 + 2x^2, b(x) = 2 + x \in \mathbb{R}[x]$ מצא $d = \gcd(a, b)$ ומצא $p, q \in \mathbb{R}[x]$ כך ש $ap + qb = d$

(ב) נגדיר: $a(x) = 7x^7 + 6x^6 + 5x^5 + 4x^4 + 3x^3 + 2x^2 + x, b(x) = x^3 + x^2 \in \mathbb{R}[x]$ מצא $d = \gcd(a, b)$ ומצא $p, q \in \mathbb{R}[x]$ כך ש $ap + qb = d$

5.

(א) יהא $f(x) \in \mathbb{F}[x]$ פולינום עם $2 \leq \deg(f) \leq 3$. הוכיחו כי $f(x)$ ראשוני אמ"מ ל $f(x)$ אין שורש (שורש של $f(x)$ הוא $a \in \mathbb{F}$ המקיים $f(a) = 0$)

(ב) הראו שיש בדיוק פולינום אי-פריק אחד ממעלה שניים ב $\mathbb{Z}_2[x]$.

(ג) העזרו בסעיף א כדי לקבוע האם $x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$ פריק.

(ד) העזרו בסעיף א כדי לקבוע האם $x^5 + x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ פריק.