

## תרגיל מספר 10 מבנים אלגבריים

### שיעורי בית 10

1.

(א) הוכיחו כי  $f(x) = x^2 + x + 4 \in \mathbb{Z}_{11}[x]$  ראשוני ולכן  $\mathbb{F} = \mathbb{Z}_{11}[x]/\langle x^2 + x + 4 \rangle$  שדה.

(ב) מצאו  $[3x + 2]^{-1}$  ב  $\mathbb{F}$  הנ"ל.

2.

(א) יהא  $\mathbb{F}$  שדה. יהיו  $a, b \in \mathbb{F}$  שונים מאפס. הוכיחו כי  $ab \neq 0$

(ב) יהא  $\mathbb{F}$  שדה סופי עם  $p^t$  איברים עבור  $p$  ראשוני ו  $t$  טבעי. נגדיר  $K = \{1, 1+1, 1+1+1, \dots\} = \{1n : n \in \mathbb{N}\}$  (כלומר  $2 = 1+1, 3 = 1+1+1, \dots$ ) וכו' הוכיחו כי  $K$  שדה עם מספר  $p$  איברים.

(ג) יהא  $\mathbb{F}$  שדה סופי ויהא  $K = \{1, 1+1, 1+1+1, \dots\}$  מסעיף קודם בעל  $p$  איברים כאשר  $p$  ראשוני. הוכיחו כי מספר האיברים ב  $\mathbb{F}$  הוא  $p^n$  עבור  $n$  טבעי. הדרכה: חישבו על  $\mathbb{F}$  כמרחב וקטורי מעל  $K$

3. יהא  $\mathbb{F}$  שדה סופי עם  $p^n$  איברים עבור  $p$  ראשוני ו  $n$  טבעי ויהא  $K = \{1, 1+1, 1+1+1, \dots\}$  משאלה קודמת. יהא  $p(x) = x^{p^n} - x \in K[x]$  ויהא  $f(x) \in K[x]$  אי פריק מתוקן שמחלק את  $p(x)$ .

(א) הוכיחו כי קיים  $a \in \mathbb{F}$  המקיים כי  $f(a) = 0$ .

(ב) נסמן ב  $q(x) \in K[x]$  את הפולינום המתוקן עם הדרגה המינימאלית המקיים  $q(a) = 0$  וששונה מפולינום האפס. הוכיחו כי  $q(x) = f(x)$ .

(ג) הוכיחו כי  $K[a] = \{q(a) : q(x) \in K[x]\}$  הוא תת שדה של  $\mathbb{F}$

(ד) הוכיחו כי מספר האיברים ב  $K[a]$  שווה ל  $p^{\deg(f)}$

(ה) הסיקו/הוכיחו כי הדרגה של  $p$  מחלקת את  $n$ .

4. יהי  $\mathbb{F} = \mathbb{F}_{2^n}$  שדה סופי הוא מקיים כי  $1 + 1 = 0$ . הוכיחו כי כל איבר בו הוא ריבוע כלומר  $\forall x \in \mathbb{F} \exists y \in \mathbb{F} : x = y^2$ .  
הדרכה: נגדיר העתקה  $\phi : \mathbb{F} \rightarrow \mathbb{F}$  ע"י  $\phi(x) = x^2$  הראו שהעתקה זו היא חח"ע והסיקו כי  $\phi$  על ולכן הטענה מתקיימת.

5. יהא  $\mathbb{F} = \mathbb{F}_{p^n}$  שדה עם  $p^n$  איברים. הוכיחו כי

$$x^{p^n-1} - 1 = \prod_{\alpha \in \mathbb{F}^\times} (x - \alpha)$$

כאשר השיוון הוא שיוון פולינומים ו  $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ .  
הסיקו את משפט וילסון: יהא  $p$  מספר ראשוני אי זוגי אזי

$$(p-1)! \equiv -1 \pmod{p}$$