

# מבנים אלגבריים - תירגול 11

10 בינואר 2016

המטרה: לבנות שדות סופיים.  
עובדה: עבור  $p$  ראשוני  $\mathbb{Z}_p$  הוא שדה עם  $p$  איברים. ראינו כי  $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$  הוא קבוצת המנה של יחס השקילות על  $\mathbb{Z}$  המוגדר  $a - b \in p\mathbb{Z} \iff a - b \in p\mathbb{Z} \iff p|a - b \iff a \equiv b$ .  
תכונות שבעזרתם מוכיחים כי  $\mathbb{Z}_p$  שדה:

1. (חלוקה עם שארית) לכל  $a, b \in \mathbb{N}$  כך ש  $b \neq 0$  קיים  $r, q$  כך ש

$$a = qb + r$$

המקיימים  $r < b$  או  $r = 0$ . והם יחידים.

2. הגדרה מספר  $n$  טבעי יקרא פריק אם ניתן להציגו כמכפלה

$$n = ab$$

כאשר  $1 < a, b < n$ .  $p$  ראשוני הוא אי פריק = לא פריק.

3. (קיום gcd) לכל 2 שלמים  $a, b$  קיים  $d = \gcd(a, b)$  המקיים

$$d | a, b \text{ (א)}$$

$$\text{(ב) אם } d' | a, b \text{ אז } d' \leq d.$$

בנוסף קיימים  $m, n$  כך ש

$$d = an + bm$$

## שדות סופיים עם $p^n$ איברים:

השדה עם  $p^n$  איברים ( $p$  ראשוני,  $n$  טבעי) הוא  $\mathbb{F} = \mathbb{Z}_p[x]/\langle f(x) \rangle$  כאשר  $\mathbb{Z}_p[x]$  הוא חוג הפולינומים מעל  $\mathbb{Z}_p$ ,  $f(x)$  הוא פולינום אי פריק מדרגה  $n$  ו  $\mathbb{F}$  הוא קבוצת המנה של יחס השקילות על  $\mathbb{Z}_p[x]$  המוגדר  $a - b \in \langle f \rangle \iff f|a - b \iff a - b \in \langle f \rangle = \{fg | g \in \mathbb{Z}_p[x]\}$ .  
תכונות דומות מתקיימות גם פה:

1. משפט (חילוק פולינומים): יהא  $\mathbb{F}$  שדה.  $\mathbb{F}[x]$  חוג הפולינומים. אזי לכל  $a(x), b(x) \in \mathbb{F}[x]$  כך ש  $b(x) \neq 0$  קיים  $r(x), q(x)$  כך ש

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

המקיימים  $deg(r) < deg(q)$  או  $r = 0$ . והם יחידים.

2. פולינום  $n(x)$  יקרא פריק אם ניתן להציגו כמכפלה

$$n = ab$$

כאשר  $0 < deg(a), deg(b) < n$ .  $f(x)$  ראשוני הוא אי פריק = לא פריק.

3. (קיום gcd): יהא  $\mathbb{F}$  שדה.  $\mathbb{F}[x]$  חוג הפולינומים. אזי לכל  $a(x), b(x) \in \mathbb{F}[x]$  קיים  $d(x) = \gcd(a, b)$  המקיים

$$d \mid a, b \quad (\text{א})$$

$$\text{deg}(d') \leq \text{deg}(d) \text{ אם } d' \mid a, b \quad (\text{ב})$$

(ג) הפולינום  $d$  מתוקן.

בנוסף קיימים  $m, n$  כך ש

$$d = an + bm$$

דוגמא:  $a(x) = 1 + 2x^2, b(x) = 2 + x$  חלק את  $a$  ב  $b$   
פתרון

$$a(x) = b(x) \cdot (x^3 + x^2 - 1) + (2x + 2)$$

ע"י חילוק פולינומים ארוך  
מצא את gcd שלהם:

$$a(x) = b(x) \cdot (x^3 + x^2 - 1) + (2x + 2)$$

$$b(x) = (2x + 2) \frac{1}{2} + 1$$

$$(2x + 2) = 1(2x + 2) + 0$$

מכאן ש  $\gcd(a, b) = 1$  כלומר זרים. נציג אותו כצירוף לינארי שלהם. נחזור אחורה

$$1 = b(x) - (2x + 2) \frac{1}{2}$$

$$= b(x) - [a(x) - b(x) \cdot (x^3 + x^2 - 1)] \frac{1}{2}$$

$$= b(x) \left[ 1 + \frac{1}{2}(x^3 + x^2 - 1) \right] - \frac{1}{2}a(x)$$

