

## מבנים אלגבריים - תירגול 13

17 בינואר 2016

הגדרה: פולינום  $p(x) \in \mathbb{F}[x]$  יקרא פריק אם ניתן להציגו כ

$$p(x) = a(x)b(x)$$

עם פולינומים  $a(x), b(x)$  מדרגה קטנה ממש מדרגת  $p(x)$ .  
הגדרה: פולינום  $p(x) \in \mathbb{F}[x]$  יקרא אי פריק אם הוא לא פריק. (אנלוגי למספר  $n$ :  $n$  יקרא פריק אם  $n = ab$  עם  $1 < a, b < n$  ויקרא אי פריק אם הוא ראשוני). למשל  $x^2 + 1 \in \mathbb{R}[x]$

### שדות סופיים

טרימנולוגיה: יהיו  $a(x), p(x) \in \mathbb{F}[x]$  שני פולינומים.  $a(x) \bmod p(x)$  מתייחס לפולינום השארית  $r(x)$  בחלוקת הפולינומים

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

בניה: נאמר כי  $a(x)$  מתייחס ל  $b(x)$  אם הם שווים מודולו  $p(x)$ . יחס זה הוא יחס שקילות. בתירגול זה נסמן את מחלקת השקילות  $\bar{a}$ .  
משפט: יהא  $\mathbb{F}$  שדה סופי. אזי הגודל שלו הוא  $p^n$  עבור  $p$  ראשוני ו  $n$  טבעי.  
המשפט הבא מוכיח את הכיוון ההפוך: עבור  $p$  ראשוני ו  $n$  טבעי קיים שדה עם  $p^n$  איברים. משפט (בנית שדות סופיים): יהא  $\mathbb{F} = \mathbb{Z}_p$  שדה עם  $p$  איברים.  $\mathbb{F}[x]$  חוג הפולינומים.  $p(x) \in \mathbb{F}$  פולינום אי פריק ממעלה  $n$  אזי

$$\mathbb{F}[x]/\langle p(x) \rangle = \{\bar{a} \mid a \in \mathbb{F}[x]\}$$

הוא שדה עם  $p^n$  עם חיבור  $\bar{a} + \bar{b} = \overline{a+b}$  וכפל  $\bar{a} \cdot \bar{b} = \overline{ab}$ .  
דוגמא: נבנה שדה עם  $2^3 = 8$  איברים. נבחר את הפולינום  $p(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ .  
איך יודעים שהוא אי פריק? כי אם היה פריק אזי היה לו שורש אבל  $p(0) = p(1) = 1 \neq 0$ .  
לפי המשפט - הקבוצה

$$\mathbb{F}_8 = \{a + bx + cx^2 \mid a, b, c \in \mathbb{Z}_2\}$$

היא שדה ביחס לפעולות חיבור וכפל מודול  $p(x)$ . שימו לב שבקבוצה מופיעים נציגים של מחלקות השקילות ולא מחלקות השקילות עצמם. לא נקפיד על ההבחנה הזאת. שימו לב כי  $x^3 = -x - 1 = x + 1$  דוגמא לפעולות:

1. חיבור/חיסור: יהא  $1 + x, 1 + x^2 \in \mathbb{F}_8$  אזי החיבור שלהם הוא  $x + x^2$ . הנגדי של  $1 + x + x^2$  הוא עצמו כי  $1 + x + x^2 = 0$

2. כפל הכפל של  $1+x$ ,  $1+x^2$  הוא

$$(1+x)(1+x^2) = 1+x+x^2+x^3 = 1+x+x^2+x+1 = x^2 + x^2 \cdot x^2 = x^4 = xx^3 = x(1+x) = x+x^2$$

דוגמא נוספת:

3. הופכי. מה ההופכי של  $a(x) = 1+x$ ? פתרון: כיוון ש  $p(x)$  אי פריק אז  $\gcd(p(x), a(x)) = 1$ . נמצא צירוף לינארי שלהם שיתן 1

$$x^3 + x + 1 = (1+x)(x^2 + x) + 1$$

כלומר  $p(x) + (x^2 + x)a(x) = 1$  מודולו  $p(x)$  נקבל כי  $(x^2 + x)a(x) = 1$  ולכן  $a(x)^{-1} = x^2 + x$  אכן מתקיים

$$(x^2 + x)(1+x) = x^2 + x + x^3 + x^2 = x + x^3 = x + 1 + x = 1$$