

תרגול 14 שדות סופיים

30 ביוני 2021

תזכורת: חוג מנה $R = \mathbb{F}[x]/\langle f \rangle = \{g + \langle f \rangle \mid g \in \mathbb{F}[x]\}$ במקום לרשום איבר בצורה $g + \langle f \rangle$ רושמים פשוט $[g]$. חיבור:

$$[g] + [h] = [g + h]$$

כפל:

$$[g][h] = [gh] = gh + \langle f \rangle$$

איבר האפס הוא $[0]$, איבר היחידה הוא $[1]$.
תרגילים:

1. נסמן $\mathbb{F} = \mathbb{Z}_5[x]/\langle p(x) = x^3 + x + 1 \rangle$.

(א) הוכיחו: \mathbb{F} שדה. כמה איברים יש בו?

פתרון: חוג מנה מצורה זו הוא שדה, אמ"ם $p(x)$ אי-פריק. בשיעורי הבית הוכחתם שפולינום ממעלה 2 או 3 הוא אי-פריק אמ"ם אין לו שורשים בשדה. אצלנו:

$$p(0) = 1 \neq 0$$

$$p(1) = 3 \neq 0$$

$$p(2) = 11 \equiv (1 \pmod{5}) \neq 0$$

$$p(3) = 1 \neq 0$$

$$p(4) = 69 \neq 0$$

אין שורשים בשדה, ולכן p אי-פריק, ולכן \mathbb{F} שדה. תראו בשיעורי הבית שבמקרה זה מתקיים:

$$|\mathbb{F}| = 5^{\deg(p)} = 5^3$$

(ב) מצאו את ההופכי של $[f(x) = x^2 + x + 1]$ בשדה זה. פתרון: ראשית, מכיון ש- $x^3 + x + 1$ אי-פריק, אז $\gcd(p, f) = 1$. לכן, ניתן למצוא $a, b \in \mathbb{Z}_5[x]$ כך ש:

$$1 = ap + bf$$

כעת נשים לב שנוכל לעבור למחלקות:

$$[1] = [ap + bf] = [a] \underbrace{[p]}_{=[0]} + [b][f]$$

(כאשר $[p] = [0]$ מכיון ש- $\langle p \rangle = [0]$). ומכאן:

$$[1] = [b][f]$$

ולכן (מכיון שמדובר בחוג חילופי אז ההפיכות היא מימין ומשמאל גם), ולכן:

$$[f]^{-1} = [b]$$

נותר למצוא את b . זה נובע מהאלגוריתם, כמו שפתרתם כבר בתרגילי בית כלשהם, וכן עשינו במסודר בתרגול של אתמול:

$q_1(x) = x + 4$	
$x^3 + x + 1$	$x^2 + x + 1$
$x^3 + x^2 + x$	
↓	
$4x^2 + 1$	
$4x^2 + 4x + 4$	
↓	
$r_1(x) = x + 2$	

כעת צריך להמשיך:

$$\begin{array}{r|l}
 q_2(x) = x + 4 & \\
 \hline
 x^2 + x + 1 & x + 2 \\
 x^2 + 2x & \\
 \downarrow & \\
 4x + 1 & \\
 4x + 3 & \\
 \downarrow & \\
 r_2(x) = 3 &
 \end{array}$$

ובסה"כ:

$$b = 2x^2 + x + 4$$

2. מצאו שדה עם 8 איברים, בו יש פתרון למשוואה $X^3 + X + 1 = 0$. פתרון: ראשית, שדה סופי הוא תמיד מסדר p^k עבור p ראשוני. לכן, שדה עם שמונה איברים הוא בעצם שדה עם 2^3 איברים. איך מקבלים כזה שדה? אמרנו, ש-

$$\mathbb{Z}_p[x]/\langle f \rangle$$

הוא שדה אמ"ם p , f ראשוניים. אצלנו ניקח $f(x) = x^3 + x + 1$ שהוא אי-פריק כי אין לו שורש:

$$f(0) = f(1) = 1$$

ולכן

$$\mathbb{Z}_2[x]/\langle f \rangle$$

שדה עם $2^3 = 8$ איברים. כעת נמצא פתרון למשוואה בשדה זה. נשים לב שעבור $[x^3 + x + 1] \in \mathbb{Z}_2[x]/\langle f \rangle$ נקבל:

$$\underbrace{[x^3 + x + 1]^3 + [x^3 + x + 1] + [1]}_{=[0]+[0]=[0]} = [1] \neq [0]$$

ולכן זה לא עובד. אלא ניקח את $[x] \in \mathbb{Z}_2[x]/\langle f \rangle$, ואז נקבל:

$$[x]^3 + [x] + [1] = [x^3 + x + 1] = \langle f \rangle = [0]$$

3. יהא $0 \neq p(x) \in \mathbb{F}[x]$ פולינום ממעלה n . הוכיחו שיש לו לכל היותר n שורשים בשדה.

פתרון: באינדוקציה: עבור $n = 0$ אז מקבלים פולינום קבוע, ואין לו שורשים ובפרט יש לו לכל היותר 0 שורשים. נניח נכונות עד n ונוכיח עבור $n + 1$: יהי p ממעלה $n + 1$. נחלק למקרים:

אם ל- p אין שורשים, אז יש לו לכל היותר $n + 1$ שורשים. אחרת יש לו לפחות שורש אחד, כלומר קיים $a \in \mathbb{F}, f(x) \in \mathbb{F}[x]$ כך ש:

$$p(x) = (x - a) \cdot f(x)$$

כמובן $\deg(f) = n$, ולכן מהנחת האינדוקציה ל- f יש לכל היותר n שורשים בשדה, וביחד עם השורש a יש לכל היותר $n + 1$ שורשים בשדה.