

פתרון תרגיל בית 7 - תורת גלואה סמסטר א', תשע"ז

שאלה 1. כמה פולינומים אי-פריקים מדרגה 8 יש מעל \mathbb{Z}_2 ?

פתרון. הפולינומים האי-פריקים מדרגה 8 מחלקים את $x^{2^8} - x$.
 $x^{2^8} - x$ הוא מכפלה של כל הפולינומים האי-פריקים מדרגה 1, 2, 4, 8 ולכן נחשב באינדוקציה:
 מכפלת הפולינומים האי-פריקים מדרגה 1: $x^{2^1} - x = x(x - 1)$ נותנים דרגה 2.
 מכפלת הפולינומים האי-פריקים מדרגה 2: היא בדיוק $\frac{x^{2^2} - x}{x(x - 1)}$ ולכן נותנים דרגה $4 - 2 = 2$
 מכפלת הפולינומים האי-פריקים מדרגה 4: היא $\frac{x^{2^4} - x}{x(x - 1)(\text{irreducible of degree 2})}$ ולכן נותנים דרגה $2^4 - 2 - 2 = 12$
 מכפלת הפולינומים האי-פריקים מדרגה 8 היא $\frac{x^{2^8} - x}{x(x - 1)(x^2 + \dots)(\text{irreducible of degree 4})}$ מדרגה $2^8 - 2 - 2 - 12 = 2^8 - 2^4$
 ולכן מספר הפולינומים האי-פריקים מדרגה 8 הוא $\frac{2^8 - 2^4}{8} = 2^5 - 2 = 30$

שאלה 2. נתון הפולינום $f(x) = x^5 - 5$ מעל \mathbb{Z}_{11} .

אם $a \notin \mathbb{Z}_{11}$ הוא שורש של הפולינום $f(x)$, מהם שאר השורשים?
 האם $f(x)$ פריק או אי-פריק מעל \mathbb{Z}_{11} ? נמקו.

פתרון. מכיוון שחבורת גלואה נוצרת ע"י אוטומורפיזם פרוביניוס $x \mapsto x^{11}$
 השורשים הם בדיוק כל הצמודים של a : $a, a^{11}, a^{11^2}, a^{11^3}, a^{11^4}$

שאלו בעצם

$$\begin{aligned}a &= a \\ a^{11} &= 3a \\ a^{11^2} &= 9a \\ a^{11^3} &= 5a \\ a^{11^4} &= 4a\end{aligned}$$

שימו לב שקיבלנו 5 שורשים שונים.
זהו פולינום ספרבילי וחבורת גלואה פועלת על קבוצת השורשים טרנזיטיבית ולכן הוא אי-פריק (לפי תרגיל קודם).

שאלה 3. נתונים פולינומים אי-פריקים $f(x), g(x) \in \mathbb{Z}_2[x]$ כך ש $\deg(f) = 6$ ו $\deg(g) = 4$.
מהו שדה הפיצול של fg מעל \mathbb{Z}_2 ?

פתרון. נסמן ב E_f את שדה הפיצול של $f(x)$, הוא שדה מגודל 2^6 .
נסמן ב E_g את שדה הפיצול של $g(x)$, הוא שדה מגודל 2^4 .
שדה הפיצול של המכפלה הוא הקומפוזיטום $E_f E_g$ - נחשב אותו:
 $E_f E_g \subseteq F_{2^{12}}$ ולכן $f, g \mid x^{2^{12}} - x$
נזכר שהתת שדות של שדה מגודל p^n הם רק השדות מגודל p^d עבור $d \mid n$ (ויש תת-שדה יחיד כזה לכל d מכיוון שכל תת-שדה כזה יהיה שדה הפיצול של $x^{p^d} - x$).
ולכן $12 \mid [E_f E_g : \mathbb{Z}_2]$
מצד שני $4, 6 \mid [E_f E_g : \mathbb{Z}_2] \Leftarrow 12$
קבלנו $[E_f E_g : \mathbb{Z}_2] = 12$ ולכן $E_f E_g = F_{2^{12}}$.

שאלה 4. 1. בנו במפורש את השדה F_{32} .

2. כמה גורמים אי-פריקים יש לפולינום $x^{64} - x$ מעל F_2 ? (אין צורך למצוא את הגורמים)

3. כמה גורמים אי-פריקים יש לפולינום $x^{64} - x$ מעל F_4 ? (אין צורך למצוא את הגורמים)

פתרון. 1. $23 = 2^5$ ולכן נחפש פולינום אי-פריק מדרגה 5 מעל F_2 . הפולינומים האי-פריקים היחידים מדרגה 1 או 2 הם $x, x+1, x^2+x+1$ (למה? ראו שאלה 1). נקח את הפולינום $f(x) = x^2(x+1)(x^2+x+1) + 1$ הוא אי-פריק כי הוא לא מתחלק באף אחד מהפולינומים הנ"ל. אם כן $F_2[x]/\langle f(x) \rangle$ הוא שדה מגודל 2^5 כדרוש. (יש עוד חמישה פתרונות אפשריים...)

2. $x^2 - x$ הוא מכפלת כל הפולינומים האי-פריקים מדרגות: 1, 2, 3, 6.
 כמות הא"פ מדרגה 1 היא 2 כי $x^2 - x = x(x + 1)$.
 כמות הא"פ מדרגה 2 היא 1 כי $\frac{x^2 - x}{x^2 - x}$ מדרגה 2.
 כמות הא"פ מדרגה 3 היא 2 כי $\frac{x^2 - x}{x^2 - x}$ מדרגה 6 ולכן יש $\frac{6}{3} = 2$ פולינומים מדרגה 3.
 כמות הא"פ מדרגה 6 היא 6 כי $\frac{x^2 - x}{(deg = 2 + 2 + 6)}$ מדרגה 54 ולכן יש $\frac{54}{6} = 9$ פולינומים.
 סך הכל יש $2 + 1 + 2 + 9 = 14$ גורמים אי-פריקים מעל F_2 .

3. $x^3 - x$ הוא מכפלת כל הפולינומים האי-פריקים מדרגות: 1, 3.
 כמות הא"פ מדרגה 1 היא 4 כי $x^3 - x$ מדרגה 4.
 כמות הא"פ מדרגה 3 היא 20 כי $\frac{x^3 - x}{x^3 - x}$ מדרגה 60 ולכן יש $\frac{60}{3} = 20$ פולינומים מדרגה 3.
 סך הכל יש $20 + 4 = 24$ גורמים אי-פריקים מעל F_4 .

שאלה 5. הוכיחו כי לכל פולינום $f(x) \in \mathbb{Z}_p[x]$ מתקיים

$$f(x)^{p^m} = f(x^{p^m})$$

עבור $m \geq 0$.

פתרון. עבור $m = 0$ זה ברור.

נראה עבור $m = 1$ ומשם הטענה נכונה באינדוקציה.

$$f(x)^p = f(x^p)$$

$$\text{נרשום } f(x) = a_0 + a_1x + \dots + a_nx^n \text{ אזי}$$

$$\begin{aligned} f(x)^p &= (a_0 + a_1x + \dots + a_nx^n)^p = a_0^p + a_1^p x^p + \dots + a_n^p (x^n)^p \\ &= a_0 + a_1x^p + \dots + a_n(x^p)^n = f(x^p) \end{aligned}$$

המעבר השני נובע מכך שבפיתוח המלא לכל שאר המחברים יש גורם p ולכן הם מתאפסים.

המעבר השלישי נכון כי לכל איבר $a \in \mathbb{Z}_p$ מתקיים $a^p = a$.