

אלגברה מופשטת 3 – תרגול 10

ספירת פולינומים אי-פריקים מעל שדה סופי:

- א. כמה גורמים אי פריקים יש ל- $x^{64} - x$ מעל \mathbb{F}_2 ? (אין צורך למצוא את הגורמים)
 ב. כמה גורמים אי פריקים יש ל- $x^{64} - x$ מעל \mathbb{F}_4 ? (אין צורך למצוא את הגורמים)

פתרון:

נסמן ב- $n_q(k)$ את מספר הפולינומים האי פריקים ממעלה k מעל \mathbb{F}_q . לפי משפט מכפלת כל הפולינומים האי פריקים המתוקנים ממעלה k היא $x^{q^k} - x$, לכן, $q^k = \sum_{d|k} dn_q(d)$ ובנוסף, מספר הגורמים האי פריקים של $x^{q^k} - x$ הוא $\sum_{d|k} n_q(d)$.

$$\mu(n) = \begin{cases} 1 & n=1 \\ 0 & a^2 | n, a > 1 \\ (-1)^k & n = p_1 \cdots p_k, p_i \neq p_j \end{cases} \quad \text{כאשר } \mu(n) \text{ היא פונקצית מביוס } , n_p(t) = \frac{\sum_{d|t} \mu\left(\frac{t}{d}\right) p^d}{t}$$

$$\text{מביוס: אם } g(n) = \sum_{d|n} f(d) \text{ כאשר } f(n), g(n) : \mathbb{N} \rightarrow \mathbb{Z} \text{ אזי } f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

$$(\text{הראו ש } \varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d)$$

א. מתקיים $n_2(1) = 2$ (ברור).

$$n_2(2) = \frac{2^2-2}{2} = 1 \text{ ולכן } 2^2 = n_2(1) + 2n_2(2) = 2 + 2n_2(2)$$

$$n_2(3) = \frac{2^3-2}{3} = 2 \text{ ולכן } 2^3 = n_2(1) + 3n_2(3) = 2 + 3n_2(3)$$

$$n_2(3) = \frac{2^6-10}{6} = 1 \text{ ולכן } 2^6 = n_2(1) + 2n_2(2) + 3n_2(3) + 6n_2(6) = 2 + 2 + 6 + 6n_2(6)$$

9.

לכן, מספר הגורמים של $x^{64} - x$ מעל \mathbb{F}_2 הוא

$$n_2(1) + n_2(2) + n_2(3) + n_2(6) = 2 + 1 + 2 + 9 = 14$$

ב. מתקיים $n_4(1) = 4$ (ברור).

$$n_4(3) = \frac{4^3-4}{3} = 20 \text{ ולכן } 2^4 = n_4(1) + 3n_4(3) = 4 + 3n_4(3)$$

$$n_4(1) + n_4(3) = 4 + 20 = 24 \text{ הוא } \mathbb{F}_4 \text{ מעל } x^{64} - x$$

דוגמא:

שלב א' מימוש הרחבת גלואה עם חבורה S_n : החבורה S_n פועלת על השדה $F(x_1, \dots, x_n)$ ע"י תמורה על האינדקסים של המשתנים x_1, \dots, x_n . בנוסף, ניתן לראות שכל איבר של S_n פועל כאוטומורפיזם של השדה.

כעת ניתן להסתכל על השדה המייצב על ידי החבורה $S_n : S = F(x_1, \dots, x_n)^{S_n}$. הפונקציות הרציונליות בו הן בדיוק אלה אשר אינוריאנטיות תחת פעולת S_n , פונקציות כאלה נקראות פונקציות סימטריות.

משפט: אם $F = E^G$ אזי $G = Gal(E/F)$

לכן $Gal(F(x_1, \dots, x_n)/S) \cong S_n$.

כעת ניתן לממש כל ת"ח של S_n כהרחבת גלואה: כי אם $H \leq S_n$ אזי $F(x_1, \dots, x_n)^H / F(x_1, \dots, x_n)$ היא הרחבת גלואה, וחבורת גלואה שלה היא H . ולפי משפט קיילי- ניתן לממש כל חבורה סופית כחבורת גלואה.

תרגיל: ידוע כעת ש $F(x_1, \dots, x_n)/S$ היא הרחבת גלואה, ולכן היא שדה פיצול של פולינום מעל S . מצאו פולינום $f(t) \in S[t]$ כך ש $F(x_1, \dots, x_n)$ הוא שדה הפיצול שלו.

פתרון: פולינום מתאים הוא $f(t) = (t-x_1) \cdots (t-x_n)$, ברור ש $F(x_1, \dots, x_n)$ הוא שדה הפיצול שלו, אבל צריך להראות ש $f(t) \in S[t]$. זה נכון כי $f(t) \in F(x_1, \dots, x_n)[t]$ אבל כל מקדמי הפולינום נקבעים ע"י האוטומורפיזמים ב S_n , ולכן $f(t) \in S[t]$.

תרגיל:

תהי E/F הרחבת גלואה. ויהיו B, C שדות ביניים מדרגות $2^b, 2^c$ בהתאמה (כך ש $b, c \geq 1$).

האם בהכרח $B \vee C$ מדרגה 2^d ?

פתרון: נראה דוגמא נגדית.

נתרגם את הבעיה לתורת החבורות: $2^b = [B:F] = [G:H]$ וגם $2^c = [C:F] = [G:K]$ עבור חבורות מתאימות $H, K \leq G = Gal(E/F)$. כבר ראינו שמתקיים $[B \vee C : F] = [G : H \cap K]$. כעת קל יותר לבנות דוגמא נגדית: ניקח $G = S_4$ שהיא חבורת גלואה של שדות מתאימים E/F . ניקח שני שיכונים שונים של S_3 לתוך S_4 : H היא ת"ח התמורות שקובעות את 4, ו K היא ת"ח התמורות שקובעות את 1. אזי $H \cap K \cong S_2$ היא מסדר 2. מתקיים $[G:H] = [G:K] = 4$, אבל $[G : H \cap K] = 12 \neq 2^d$.

משפט שטייניץ: הרחבה E/F סופית היא פשוטה אם ורק אם יש לה מספר סופי של שדות ביניים.

פתרון: אם ההרחבה היא פשוטה אזי $E = F(a)$. נסמן ב $f(x) \in F[x]$ את הפולינום המינימלי של a מעל F .

נשים לב שלכל שדה ביניים $F \subset B \subset E$ מתקיים $E = B(a)$, ואם $g(x) \in B[x]$ הפולינום המינימלי של a מעל B , אזי $f(x) | g(x)$. אם b_1, \dots, b_r הם המקדמים של $g(x)$ אזי נגדיר $B' = F(b_1, \dots, b_r) \subseteq B$. ולכן הוא הפולינום המינימלי של a מעל B' . אם כך $g(x) \in B'[x]$ בהכרח אי-פריק, ולכן הוא הפולינום המינימלי של a מעל B' . אם כך

$[E = B(a) : B] = [E = B'(a) : B]$, ולכן בהכרח $B = B'$. אם כך כל שדה ביניים נקבע ע"י מחלק מתוקן של $f(x)$, אבל יש מספר סופי של מחלקים כאלה, ולכן יש מספר סופי של שדות ביניים.

נניח שמספר הרחבות הביניים הוא סופי. ידוע שכל הרחבה סופית של שדה סופית היא פרימיטיבית, ולכן ניתן להניח ש F אינסופי. $E = F(a_1, \dots, a_n)$. נראה באינדוקציה על n ש E הרחבה פשוטה. מספיק להראות ש $E = F(a_1, a_2)$ היא פשוטה. נסתכל על כל הצירופים הלינאריים $a_1 + ta_2, t \in F$, יש אינסוף כאלה, אבל לפי ההנחה יש מספר סופי של שדות $F(a_1 + ta_2)$. לכן קיימים t, t' כך ש $F(a_1 + ta_2) = F(a_1 + t'a_2) = F(a_1, a_2) = E$. כעת מתקיים $F(a_1 + ta_2) = F(a_1 + t'a_2)$ כלומר E פשוטה.

משפט האיבר הפרימיטיבי: כל הרחבה ספרבילית סופית E/F היא פשוטה.

הוכחה: קיימת הרחבת גלואה סופית K/F המכילה את E . בעלת מספר סופי של שדות ביניים, ולכן היא פשוטה.