ספירת פולינומים אי־פריקים מעל שדה סופי

מרגיל מנחה

כמה גורמים אי־פריקים יש ל$x^{64}-x$ מעל $\mathbb{F}_2$?

נסמן ב$n_q(k)$ את מספר הפולינומים האי־פריקים ממעלה k מעל $\mathbb{F}_q$.
אם f פולינום אי־פריק ממעלה k מעל $\mathbb{F}_q$ אזי הוא מחלק את $x^{q^k}-x$.
הוספת שורש של f ל$\mathbb{F}_q$: $\mathbb{F}_q(\alpha)$. אזי $[\mathbb{F}_q(\alpha):\mathbb{F}_q]=k$.
השדה $\mathbb{F}_q(\alpha)$ הוא שדה מפצל של f(כל שאר השורשים של f הם $(\alpha,\alpha^q,\ldots,\alpha^{q^{k-1}}$).
זהו שדה עם עצמה q^k ולכן כל איבריו הם שורשים של $x^{q^k}-x$.
בצורה דומה עבור כל $d\mid k$, כל פולינום אי־פריק מדרגה d מחלק גם את $x^{q^k}-x$.

טענה

מתקיים $q^k=\sum_{d|k} d\cdot n_q(d)$

זה נכון לפי סכימת הדרגות של הפולינומים האי־פריקים.

מסקנה

מספר הגורמים האי־פריקים של $x^{q^k}-x$ הוא $\sum_{d|k} n_q(d)$.

נחזור לתרגיל המנחה

במקרה שלנו $k=6$(כי $2^6=64$)

$$n_2(1)=2 \qquad n_2(2)=1$$

$$n_2(1)+2\cdot n_2(2)+4\cdot n_2(4)=2^4$$

$$2+2\cdot 1+4n_2(4)=2^4$$

$$n_2(4)=3$$

($n_2(4)$ מיותר, שכן $4\nmid 6$)

$$1\cdot n_2(1)+3\cdot n_2(3)=2^3=8 \implies n_2(3)=2$$

$$1\cdot \underbrace{n_2(1)}_{=2}+\underbrace{2\cdot n_2(2)}_{=2}+\underbrace{3\cdot n_2(3)}_{6}+6\cdot n_2(6)=64$$

$$n_2(6) = 9$$

מספר הגורמים האי־פריקים של $x^{64} - x$?

$$\sum_{d|k} n_2(d) = 14$$

נוסחת ההיפוך של מביוס

פונקציית מביוס היא $\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & a^2 \mid n, a > 1 \\ (-1)^k & n = p_1 \cdots p_k, p_i \neq p_j \end{cases}$.

אם $g(n) = \sum_{d|n} f(d)$ אזי $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

$$n_q(n) = \frac{\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d}{n}$$

משפט(שטייניץ)

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

הוכחה

אם ההרחבה E/F פשוטה, אזי $E = F(a)$. יהי B שדה ביניים. אזי $B(a) = E$.

יהי $f(x) \in F[x]$ הפולינום המינימלי של a מעל F. נסמן ב$g(x) \in B[x]$ את הפולינום המינימלי של a מעל B.

$\Longleftarrow$ $g(x) \mid f(x)$ ב$B[x]$.

נסמן ב$b_1, \ldots b_k$ את המקדמים של $g(x)$ בB. $B' = F(b_1, \ldots b_k) \subseteq B$:

$$\begin{array}{c} E \\ | \\ B \\ | \\ B' \\ | \\ F \end{array}$$

$g(x) \in B'[x]$ והוא אי־פריק שם.

$$B'(a) = E$$

$$[E : B'] = \deg g(x) = [E : B]$$

$$\implies B = B'$$

הפולינום $g(x)$ קובע את השדה. יש מספר סופי של פולינומים מתוקנים שמחלקים את $f(x)$, ולכן יש מספר סופי של שדות ביניים.

בכיוון השני: נניח שיש מספר סופי של שדות ביניים בין E לF. אפשר להניח שF שדה אינסופי(כי ראינו שהרחבה סופית של שדה סופי היא פשוטה). ההרחבה E/F סופית(לפי הנתון).

$$E = F(a_1, \dots a_n)$$

נוכיח באינדוקציה: מספיק להוכיח עבור $E = F(a_1, a_2)$. נסתכל על צירופים $a_1 + ta_2$ כאשר $t \in F$: F אינסופי ויש מספר סופי של שדות ביניים ולכן $F(a_1 + t_1 a_2) = F(a_1 + t_2 a_2)$ עבור $t_1 \neq t_2$. השדה מכיל $\begin{matrix} a_1 + t_1 a_2 \\ a_1 + t_2 a_2 \end{matrix}$ וניתן להחליף את a_1, a_2, ולכן $F(a_1 + t_1 a_2) = F(a_1, a_2)$.

משפט האיבר הפרימיטיבי

כל הרחבה סופית ספרבילית היא פשוטה.

הוכחה

$$E/F$$

$$E = F(a_1, \dots a_n)$$

לוקחים את שדה הפיצול של $f(x) = m_{a_1}(x) \cdots m_{a_n}(x)$, וזאת הרחבת גלואה של F(ניתן להחליף את f בפולינום ספרבילי).

יש לE'/F מספר סופי של שדות ביניים(לפי התאמת גלואה). לפי שטייניץ ההרחבה E'/F פשוטה.

בניית הרחבת גלואה עם חבורת גלואה סופית כלשהי

שלב א: מימוש החבורה S_n כחבורת גלואה

יהי F שדה כלשהו. שדה שברים של $K = F(x_1, \dots x_n) \leftarrow F[x_1, \dots x_n]$.

יש פעולה של S_n על K - מפעילים את התמורה של האינדקסים של הx_i. בנוסף כל תמורה היא אוטומורפיזם של K.

נגדיר $S = K^{S_n}$ שדה הפונקציות הסימטריות. לדוגמה: $x_1 + \cdots + x_n \in S$.

$$[K : S] = \left[K : S^{S_n}\right] = |S_n| = n!$$

בנוסף $\mathrm{Gal}\left(K/S\right) = S_n$.

כל חבורה סופית איזומורפית לתת חבורה של S_n(לפי קיילי). לכן אם יש לנו $H \leq S_n$, אזי $\mathrm{Gal}\left(K/K^H\right) = H$.

K הוא שדה מפצל של איזה פולינום מעל S?

$$f\left(\lambda\right) = \prod \left(\lambda - x_i\right)$$

S פועלת טריווילית על $f\left(x\right)$ ולכן $f\left(\lambda\right) \in S\left[x\right] \Longleftarrow K/S$ היא הרחבת גלואה.

S נוצר ע"י המקדמים של $f\left(\lambda\right)$ שהם <u>הפונקציות הסימטריות האלמנטריות</u>.