

אלגברה ב2

© ארזים

5 באפריל 2017

תרגיל נגדיר את הפולינום

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

הראו כי לכל m עם $\gcd(m, n) = 1$, מתקיים $n \mid f(m)$.

פתרון מהמשפט מתקיים לכל ראשוני p :

$$\frac{f(p)}{n} = \pi_p(n)$$

לכן, $n \mid f(p)$ לכל ראשוני p . ממשפט דיריכלה, שלא הוכחנו לא נוכיח, לכל m, n זרים, קיים p המקיים $p \equiv m \pmod{n}$. אזי

$$f(m) \equiv f(p) \equiv 0 \pmod{n}$$

וסיימנו.

תרגיל הוכיחו כי

$$\mathbb{F}_9 \cong \mathbb{F}_3 \left[\begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} \right] = \text{Span} \left\{ \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}^k \mid k \in \mathbb{Z} \right\}$$

פתרון נחשב פולינום אופייני:

$$\det \begin{pmatrix} x & 1 \\ 1 & x+1 \end{pmatrix} = x^2 + x + 2$$

זהו פולינום אי פריק. נגדיר הומומורפיזם:

$$\tau : \mathbb{F}_3[x] \rightarrow \mathbb{F}_3 \left[\begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} \right]$$

על ידי $\tau(x) = \begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}$. אזי $\ker \tau \subseteq (x^2 + x + 2)$, מקיילי המילטון, אבל הפולינום האופייני אי פריק, ולכן גם המינימלי - כלומר יש שוויון. אם כן

$$\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2+x+2) = \mathbb{F}_3[x]/\ker \tau \cong \mathbb{F}_3 \left[\begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix} \right]$$

תרגיל הראו כי בשדה סופי כל איבר הוא סכום של שני ריבועים.

פתרון נגדיר $\varphi: x \mapsto x^2$. זהו אנדומורפיזם של F^* . הגרעין הוא $\{\pm 1\}$, ולכן

$$F^*/\ker \varphi \cong \text{Im} \varphi$$

מכאן נובע כי

$$|\text{Im} \varphi| \geq \frac{|F^*|}{|\ker \varphi|} \geq \frac{1}{2} |F^*|$$

כעת נגדיר

$$A = \{x^2 \mid x \in F\}$$

$$B = \{a - y^2 \mid y \in F\}$$

אם כן,

$$|A| \geq \frac{|F^*|}{2} + 1 = \frac{|F| + 1}{2}$$

כמו כן, B מתקבלת מהפעלת העתקה חד־חד־ערכית ועל, ולכן $|B| = |A|$. אם כן:

$$|F| \geq |A \cup B| = |A| + |B| - |A \cap B| \geq |F| + 1 - |A \cap B|$$

$$|A \cap B| \geq 1$$

אם כן, יהי $t \in A \cap B$. קיימים, מהגדרת הקבוצות, x, y המקיימים

$$x^2 = a - y^2$$

$$a = x^2 + y^2$$

וסיימנו.

תרגיל הראו שלכל n קיימים $\lambda_0, \dots, \lambda_{n-1} \in \mathbb{C}$ כך שמתקיים

$$\sum_{k=0}^{n-1} \lambda_k e^{\frac{2\pi i k x}{n}} = \begin{cases} 1 & x = 1 \\ 0 & x \neq 1 \end{cases}$$

כאשר $0 \leq x \leq n-1$ שלם.

פתרון נגדיר לכל k את $f_k(x) = e^{\frac{2\pi i k x}{n}}$ היא פונקציה מהחבורה $\mathbb{Z}/n\mathbb{Z}$ אל $\mathbb{C}^*$, שהיא הומומורפיזם. $f_0, \dots, f_{n-1}$ הם כרקטרים שונים, לכן בלתי תלויים. אבל הם איברים במרחב הווקטורי $\mathbb{C}^{(\mathbb{Z}/n\mathbb{Z})}$, שהוא ממימד n , ולכן גם פורשים. לכן בפרט יש סקלרים שיצרו את הפונקציה המבוקשת.