אלגברה ב2

ⓒ ארזים

5 באפריל 2017

תרגיל נגדיר את הפולינום

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

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

פתרון מהמשפט מתקיים לכל ראשוני p:

$$\frac{f\left(p\right)}{n}=\pi_{p}\left(n\right)$$

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

$$f\left(m\right)\equiv f\left(p\right)\equiv0\left(\mod n\right)$$

וסיימנו.

תרגיל הוכיחו כי

$$\mathbb{F}_{9}\cong\mathbb{F}_{3}\left[\begin{pmatrix}0 & 2\\ 2 & 2\end{pmatrix}\right]=\mathrm{Span}\left\{ \begin{pmatrix}0 & 2\\ 2 & 2\end{pmatrix}^{k}\mid k\in\mathbb{Z}\right\}$$

פתרון נחשב פולינום אופייני:

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

וזה פולינום אי פריק. נגדיר הומומורפיזם:

$$\tau:\mathbb{F}_{3}\left[x\right]\to\mathbb{F}_{3}\left[\begin{pmatrix}0 & 2\\ 2 & 2\end{pmatrix}\right]$$

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

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

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

$$ {}^{F^*}\!/\!_{\ker\varphi} \cong \mathrm{Im}\varphi$$

מכאן נובע כי

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

כעת נגדיר

$$\begin{aligned} A &= \left\{x^2 \mid x \in F\right\} \\ B &= \left\{a - y^2 \mid y \in F\right\} \end{aligned}$$

אם כן,

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

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

$$\begin{aligned} |F| \geq |A \cup B| = |A| + |B| - |A \cap B| \geq |F| + 1 - |A \cap B| \\ |A \cap B| \geq 1 \end{aligned}$$

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

$$\begin{aligned} x^2 &= a - y^2 \\ a &= x^2 + y^2 \end{aligned}$$

וסיימנו.

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

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

כאשר $0\leq x\leq n-1$ שלם.

פתרון נגדיר לכל k את $f_k\left(x\right)=e^{\frac{2\pi ikx}{n}}$ 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.