פתרון מטלה 06 — מבנים אלגבריים (2), 80446

17 במאי 2025

שאלה 1

יהי $\xi_8 \in \mathbb{C}$ שורש יחידה פרימיטיבי מסדר 8.

נמצא את כל תתי־ההרחבות הריבועיות של $\mathbb{Q}(\xi_8)/\mathbb{Q}$, כלומר את כל השדות K כך ש־$\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\xi_8)$ ו־$[K:\mathbb{Q}] = 2$.

פתרון נבחין כי מחישוב ישיר,

$$\xi_8 = e^{\frac{2\pi i}{8}} = \frac{1+i}{\sqrt{2}}$$

ולכן גם,

$$\xi_8^3 = \frac{-1+i}{\sqrt{2}}$$

ונסיק כי $\xi_8 - \xi_8^3 = \sqrt{2} \in \mathbb{Q}(\xi_8)$. בנוסף מחיבור שני איברים אלה נסיק שגם $i \in \mathbb{Q}(\xi_8)$. נסיק ש־$\mathbb{Q}(\sqrt{2}, i) \subseteq \mathbb{Q}(\xi_8)$, ונרצה להראות שוויון.

אנו יודעים ש־$[\mathbb{Q}(\xi_8):\mathbb{Q}] = 4$. מצד שני גם: $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},i):\mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$. $[\mathbb{Q}(\xi_8):\mathbb{Q}] = [\mathbb{Q}(\xi_8,\xi_8^2):\mathbb{Q}(\xi_8^2)] \cdot [\mathbb{Q}(\xi_8^2):\mathbb{Q}]$, כאשר השתמשנו בעובדה ש־$\xi_8^2 = \xi_4$ (מחישוב ישיר). נסיק אם כן שקיים שוויון דרגות ולכן בהכרח $\mathbb{Q}(\xi_8) = \mathbb{Q}(\sqrt{2}, i)$.

עלינו אם כך למצוא את כל השדות $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\sqrt{2}, i)$ מדרגה 2 מעל $\mathbb{Q}$, ונבחין כבר כמסקנה ש־$\mathbb{Q}(i)$ וכן ש־$\mathbb{Q}(\sqrt{2})$ מקיימים את הטענה. מבדיקה ישירה גם $\mathbb{Q}(\sqrt{-2})$ הוא שדה כזה, ולא קיימים שדות נוספים כאלה, שכן שלושת האיברים הללו מרכיבים בסיס של $\mathbb{Q}(\xi_8)$ לפי שאלה 3 ממטלה 3.

שאלה 2

סעיף א'

נוכיח את הזהויות הנתונות לפולינומים ציקלוטומיים.

i

נניח ש־$2 \nmid n$ ונוכיח, $\Phi_{2n}(t) = \Phi_n(-t)$.

הוכחה.

$$t^{2n} - 1 = \prod_{d|2n} \Phi_d(t) = \prod_{d|n} \Phi_{2d}(t) \cdot \prod_{d|n} \Phi_d(t) = \prod_{d|n} \Phi_{2d}(t) \cdot (t^n - 1)$$

ולכן,

$$\prod_{d|n} \Phi_{2d}(t) = t^n + 1$$

מצד שני,

$$(-t)^n - 1 = \prod_{d|n} \Phi_d(-t)$$

אבל $2 \nmid n$ ולכן $(-t)^n - 1 = -(t^n + 1)$ ונסיק,

$$\prod_{d|n} \Phi_{2d}(t) = -\prod_{d|n} \Phi_d(-t)$$

ועתה נוכל להוכיח בפשטות את הטענה באינדוקציה על n, עבור $n = 1$ מתקיים,

$$\Phi_2(t) = -\Phi_1(-t)$$

עבור $n = 3$ בהתאם נובע,

$$\Phi_2(t) \cdot \Phi_6(t) = -\Phi_1(-t) \cdot \Phi_3(-t)$$

ומהמקרה $n = 1$ נסיק שהטענה חלה, עתה נניח שהטענה נכונה ל־$m < n$ ונבחן את n, נשתמש בתהליך דומה למקרה $n = 3$ ונבטל את המכפלות הקטנות, נובע ישירות,

$$\Phi_{2n}(t) = \Phi_n(-t)$$

והשלמנו את המהלך. □

ii

נניח ש־p ראשוני ונראה ש־$\Phi_{pn}(t) = \Phi_n(t^p)$ אם $p \mid n$, ואחרת $\Phi_{pn}(t) = \Phi_n(t^p)/\Phi_n(t)$.

הוכחה. אנו יודעים כי μ_{pn} חבורה ציקלית, ולכן $\zeta \in \mu_{np}$ אם ורק אם $\zeta^p \in \mu_n$, זאת ישירות מטעמי דרגה.
נסיק ש־$t - \zeta \mid \Phi_{pn}(t)$ אם וקר אם $t - \zeta^p \mid \Phi_n(t^p)$ ישירות מהגדרת Φ. □

סעיף ב'

נחשב את $\Phi_n(t)$ עבור $1 \leq n \leq 10$.

פתרון עבור $n = 1$ אנו יודעים כי $\Phi_1(t) = t - 1$ ישירות מהגדרה. אנו גם יודעים ש־$\Phi_2(t) = \frac{t^2-1}{t-1} = t + 1$. עבור $n = 3, 5, 7$ נשתמש בעובדה שהם ראשוניים ולכן,

$$\Phi_p(t) = \frac{t^n - 1}{t - 1}$$

ונקבל $\Phi_3(t) = t^2 + t + 1, \Phi_5(t) = t^4 + t^3 + t^2 + t + 1, \Phi_7(t) = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$.
עבור $n = 4$ נשתמש בעובדה ש־$\Phi_{2\cdot 2}(t) = \Phi_2(t^2)$ מתת־הסעיף הקודם ונובע ש־$\Phi_4(t) = t^2 + 1$. עבור $n = 6$ נקבל מתת־הסעיף הראשון

$\Phi_6(t) = \Phi_3(-t) = t^2 - t + 1$. עבור $n = 8$,

$$t^8 - 1 = \prod_{d|8} \Phi_d(t) \iff \Phi_8(t) = \frac{t^8 - 1}{(t-1)(t+1)(t^2-1)} = t^4 + 1$$

וכך גם,

$$\Phi_9(t) = \Phi_3(t^3) = t^6 + t^3 + 1$$

ולבסוף,

$$\Phi_{10}(t) = \Phi_5(-t) = t^4 - t^3 + t^2 - t + 1$$

שאלה 3

ראינו כי $\mathbb{F}_{p^d}/\mathbb{F}_p$ היא הרחבה ציקלוטומית על־ידי שורש יחידה ξ מסדר p^d-1.
ראינו גם כי במקרה זה יש שיכון $\mathrm{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p) \hookrightarrow \mathrm{Aut}(\mu_{p^d-1}) \simeq (\mathbb{Z}/(p^d-1)\mathbb{Z})^\times$.
אנו נתאר את השיכון,

$$\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^d}) = \mathrm{Fr}_p^{\mathbb{Z}/d\mathbb{Z}} \hookrightarrow (\mathbb{Z}/(p^d-1)\mathbb{Z})^\times$$

נבדוק מה היא תמונת איבר פרוביניוס Fr_p.

פתרון נראה כי $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^d}) \hookrightarrow \mathrm{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p)$. יהי $\sigma = \mathrm{Fr}_p^n \in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^d})$, אנו כבר יודעים כי זוהי חבורה ציקלית ובחרנו את אחד מאיבריה. נבחר $\tau \in \mathrm{Aut}(\mathbb{F}_{p^d}/\mathbb{F}_p)$ על־ידי $\tau(x) = \sigma(x)/\mathbb{F}_p$. נבחין כי מהגדרה כל σ, σ' כאלה מסכימות על $\mathbb{F}_p$, כלומר $\sigma \restriction \mathbb{F}_p = \sigma' \restriction \mathbb{F}_p$ ולכן $\tau = \tau'$ אם ורק אם $\sigma = \sigma'$, וזהו אכן שיכון. נבחין כי $\xi \mapsto \xi^{p^n}$ ב־τ על־פי ההגדרה, וזהו שיכון $\varphi \in \mathrm{Aut}(\mu_{p^d-1})$ מהגדרת ξ, וכן $\varphi \mapsto \phi$ עבור $\phi(m) = m \cdot p^n$, כפי שהגדרנו את האיזומורפיזם $\mathrm{Aut}(\mu_{p^d-1}) \simeq (\mathbb{Z}/(p^d-1)\mathbb{Z})^\times$. כלומר $\mathrm{Fr}_p^n \mapsto (m \mapsto m \cdot p^n)$ לכל $\mathrm{Fr}_p^n \in \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^d})$.

בפרט נוכל להסיק שעבור $n = 1$ מתקבל $m \mapsto pm$.

שאלה 4

תהי $q = p^k$ חזקת ראשוני. פולינום $f \in \mathbb{F}_q[x]$ מדרגה $d > 1$ נקרא פרימיטיבי אם הוא אי־פריק וכל שורש של f ב־$\mathbb{F}_{q^d}$ הוא יוצר של $\mathbb{F}_{q^d}^\times$.

סעיף א'

נמצא דוגמה לשדה סופי ולפולינום אי־פריק מדרגה $d > 1$ מעל $\mathbb{F}_q$ שאינו פרימיטיבי.

פתרון נגדיר $p = 3, k = 1$ ואת הפולינום $f(x) = x^2 + 1$, מבדיקה ישירה נקבל ש־f אי־פריק ב־$\mathbb{F}_3$.

$d = \deg_{\mathbb{F}_3} f = 2$ ולכן נבחן את שורשי f ב־$\mathbb{F}_9$.

נגדיר $\mathbb{F}_9 = \mathbb{F}_3(\xi)$ עבור ξ שורש יחידה פרימיטיבי מסדר $p^d - 1 = 8$, ונסיק ש־$f(x) = (x - \xi^4)(x - 2\xi^4)$.

נבחין כי $|\langle \xi^4 \rangle| = |\langle 2\xi^4 \rangle| = 3$ בעוד $|\mathbb{F}_{q^d}^\times| = 8$ ולכן פולינום זה לא פרימיטיבי.

סעיף ב'

נראה שאם $\alpha \in \mathbb{F}_{q^d}$ יוצר את $\mathbb{F}_{q^d}^\times$ אז המסלול שלו ב־$\mathrm{Aut}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ מכיל d איברים שונים.

הוכחה. $|\mathbb{F}_{q^d}^\times| = q^d - 1$ שכן כל איבר לא טריוויאלי הוא הפיך.

יהי $\zeta^n \in \mathbb{F}_{q^d}^\times = \mathbb{F}_q(\zeta)^\times$ עבור ζ שורש יחידה פרימיטיבי מסדר $q^d - 1$, כאשר $n \in \mathbb{Z}/(q^d - 1)\mathbb{Z}$. $\zeta \mapsto \zeta^n$ הוא אוטומורפיזם ולכן בפרט משרה $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ על־ידי $\pi(\zeta) = \pi(\zeta^n)$. נתון לנו שלכל n, קיים m כך ש־$\alpha^m = \zeta^n$ ולכן נוכל להסיק ישירות שקיים σ כך ש־$\sigma(\pi(\alpha)) = \pi(\zeta^n)$, כלומר גודל המסלול של α ב־$\mathrm{Aut}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ הוא $\varphi(q^d - 1) \geq d$. $\square$

סעיף ג'

נוכיח שיש בדיוק $\varphi(q^d - 1)/d$ פולינומים פרימיטיביים מתוקנים מדרגה d ב־$\mathbb{F}_q[x]$.

הוכחה. משאלה 3 ומהסעיף הקודם נוכל להסיק שיש $\varphi(q^d - 1)$ איברים שונים שיוצרים את $\mathbb{F}_{q^d}^\times$, זאת על־ידי בחינת השיכון ב־$\mathbb{Z}/(q^d - 1)\mathbb{Z}$.

אילו $f, g \in \mathbb{F}_q[x]$ שני פולינומים שונים כך ש־$f(\xi) = g(\xi) = 0$ עבור ξ יוצר של $\mathbb{F}_q^\times$, אז נקבל שקיים $h \mid f, g$ פולינום פרימיטיבי מדרגה קטנה מ־d. אבל נקבל ש־$\mathbb{F}_q/(h) \simeq \mathbb{F}_{q^d}$ בסתירה לדרגת h, ולכן לא קיימים פולינומים כאלה. בנוסף השורשים הם שונים כמסקנה ממשפט 5.5.11, ולכן נסיק מכמות האיברים שחייבים להיות בדיוק $\frac{\varphi(q^d-1)}{d}$ פולינומים כאלה. $\square$