פתרון מטלה 06 — מבנים אלגבריים 2, 80446

24 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 שיתקיים $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{Q}(\xi_8)$ ו־$[K:\mathbb{Q}]=2$.

הוכחה: ראשית

$$\xi_8 = \left\{e^{\frac{2k\pi i}{8}} \mid k \in \{1,3,5,7\}\ (\gcd(k,8)=1)\right\} = \left\{\frac{\sqrt{2}}{2}(1+i), \frac{\sqrt{2}}{2}(-1+i), -\frac{\sqrt{2}}{2}(1+i), \frac{\sqrt{2}}{2}(1-i)\right\}$$

מסימטרייה סביב מעגל היחידה, נבחר $\xi_8 = \frac{\sqrt{2}}{2}(1+i)$ ונקבל $i = \sqrt{2}\xi_8 - 1$ ולכן $i \in \mathbb{Q}(\xi_8), \sqrt{2} \in \mathbb{Q}(\xi_8)$ ואז $\mathbb{Q}\left(i,\sqrt{2}\right) \subseteq \mathbb{Q}(\xi_8)$, אבל $\xi_8 = \frac{1}{\sqrt{2}}(i+1)$ ולכן $\mathbb{Q}(\xi_8) = \mathbb{Q}\left(i,\sqrt{2}\right)$.
נסמן $L = \mathbb{Q}(\xi_8)$ ונחפש את כל תתי־שדות K של L כך שיתקיים $[L:K]=2$. יהי $\mathbb{Q} \subseteq K \subseteq L$ כך ש־$[K:\mathbb{Q}]=2$, זו הרחבה ריבועית ולכן קיים $d \in \mathbb{Q}$ כך ש־$K = \mathbb{Q}\left(\sqrt{d}\right)$ ולכן $L = \mathbb{Q}\left(\sqrt{-1},\sqrt{2}\right)$ וכמובן ש־$\sqrt{-1} \notin \mathbb{Q}\left(\sqrt{2}\right)$, ולכן $\left[\mathbb{Q}\left(\sqrt{-1},\sqrt{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] > 1$, אבל (-1) הוא שורש של $x^2+1 \in \mathbb{Q}\left(\sqrt{2}\right)$ ולכן $\left[\mathbb{Q}\left(\sqrt{-1},\sqrt{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] > \leq 2$ ובסך־הכל $\left[\mathbb{Q}\left(\sqrt{-1},\sqrt{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] = 2$ ואז מכפליות הדרגה נקבל שמתקיים

$$\left[\mathbb{Q}\left(\sqrt{-1},\sqrt{2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{-1},\sqrt{2}\right) : \mathbb{Q}\left(\sqrt{2}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2 \cdot 2 = 4$$

ואנחנו כבר יודעים להגיד שההרחבות

$$\mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}\left(\sqrt{-1}\right), \mathbb{Q}\left(\sqrt{-2}\right)$$

הן תתי־הרחבות ריבועיות של $\mathbb{Q}\left(\sqrt{2},i\right) = \mathbb{Q}(\xi_8)$.
משאלה 3 במטלה 3 נובע אם כך ש־$\mathcal{B} = \left\{1,\sqrt{2},\sqrt{-1},\sqrt{-2}\right\}$ הוא בסיס ל־L וכל איבר ב־L הוא מהצורה

$$a + b\sqrt{2} + ci + d\sqrt{2}i\ (a,b,c,d \in \mathbb{Q})$$

ונניח כי $\alpha \in \mathbb{Q}\left(\sqrt{2},i\right)$ כך ש־$\alpha^2 = d \in \mathbb{Q}$ וגם $\alpha \notin \mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}(i), \mathbb{Q}\left(\sqrt{-2}\right)$. אז

$$\alpha = a + b\sqrt{2} + ci + d\sqrt{2}i \iff a^2 = \left(a + b\sqrt{2} + ci + d\sqrt{2}i\right)^2$$

$$\iff \alpha^2 = a^2 - c^2 + 2\sqrt{2}ab + 2iac + 2b^2 - 2d^2 + 2\sqrt{2}iad + 2\sqrt{2}ibc + 4ibd + 2\sqrt{2}i^2cd$$

אנחנו רוצים ש־$\alpha^2 \in \mathbb{Q}$, נסדר את הביטוי לעיל

$$\alpha^2 = \underbrace{a^2 + 2b^2 - c^2 - 2d^2}_{\in\mathbb{Q}} + \underbrace{2\sqrt{2}ab - 2\sqrt{2}cd}_{\in\mathbb{Q}\left(\sqrt{2}\right)} + \underbrace{2iac + 4ibd}_{\in\mathbb{Q}(i)} + \underbrace{2\sqrt{2}iad + 2\sqrt{2}ibc}_{\in\mathbb{Q}\left(\sqrt{-2}\right)}$$

אז כדי ש־$\alpha^2 \in \mathbb{Q}$ צריך להתקיים

$$2\sqrt{2}ab - 2\sqrt{2}cd + 2iac + 4ibd + 2\sqrt{2}iad + 2\sqrt{2}ibc = 0$$

ואז יש לנו את המערכת

$$ab = cd,\ \ ac = -2bd, ad = -bc$$

נפתור ונקבל שיש תלות מלאה ביניהם ולכן יש לנו 4 מצבים אפשריים

1. $a = b = c = 0$ ואז ניתן לבחור d ונקבל $\alpha = d\sqrt{2}i \Rightarrow \alpha^2 = -2d^2$
2. $a = b = d = 0$ ואז ניתן לבחור c ונקבל $\alpha = ci \Rightarrow \alpha^2 = -c^2$
3. $a = c = d = 0$ ואז ניתן לבחור b ונקבל $\alpha = b\sqrt{2} \Rightarrow \alpha^2 = 2b^2$
4. $c = d = b = 0$ ואז ניתן לבחור a ולקבל $\alpha = a \in \mathbb{Q}$ וזה לא פיתרון אפשרי להרחבה ריבועית

אבל כל הפתרונות האלו הם עדיין בתוך $\mathbb{Q}(i), \mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}\left(\sqrt{-2}\right)$.
שאר הפתרונות הלא טריוויאלים שנקבל יביאו לנו את התלויות

$$c^2 = -2b^2, d^2 = -b^2, a^2 = 2b^2$$

וגם הם רק בתוך ההרחבות שמצאנו כבר אם ניקח שורשים.
ולכן התתי־הרחבות המבוקשים הם רק $\mathbb{Q}\left(\sqrt{2}\right), \mathbb{Q}(i), \mathbb{Q}\left(\sqrt{-2}\right)$. $\square$

שאלה 2

סעיף א'

נוכיח את הזהויות הבאות של פולינומים ציקלוטומים.

תת־סעיף א'

אם $n > 1$ אי־זוגי אז $\Phi_{2n}(t) = \Phi_n(-t)$.

הוכחה: אנחנו יודעים ששורשי היחידה הפרימטיביים מסדר n נתונים על־ידי $e^{\frac{2\pi i k}{n}}$ עבור $\gcd(k,n) = 1$.

באותו אופן, שורשי היחידה הפרימיטיביים מסדר $2n$ נתונים על־ידי $e^{\frac{2\pi i \ell}{2n}}$ עבור $\gcd(\ell, 2n) = 1$.

עכשיו, אם $\gcd(k,n) = 1$ אז גם $\gcd(2k+n, 2n) = 1$. למה? כי אם נסמן $d = \gcd(2k+n, 2n)$ אז $d \mid 2n, d \mid (2k+n)$, ולכן בפרט $d \mid (2k+n) - n = 2k$ כי הוא מחלק גם כל צירוף לינארי שלהם. לכן $d \mid 2k, d \mid 2n$ ולכן גם $d \mid (2k, 2n) = 2\gcd(k,n) = 2$ ולכן $d \in \{1,2\}$ בלבד. נראה ש־$d \neq 2$. נניח שלא, ולכן מתקיים

$$2 \mid (2k+n) \Rightarrow 2k+n \equiv 0 (\operatorname{mod} 2) \Rightarrow n \equiv -2k \equiv 0 (\operatorname{mod} 2) \Rightarrow n \equiv 0 (\operatorname{mod} 2) \Rightarrow 2 \mid n$$

אבל מהנתון $n > 1$ הוא אי־זוגי, וזאת סתירה ולכן $\gcd(2k+n, 2n) = 1$.

אז מתקיים

$$\Phi_{2n}(t) = \prod_{\gcd(k,n)=1} \left(t - e^{\frac{2\pi i(2k+n)}{2n}}\right) \underset{e^{\pi i} = -1}{=} \prod_{\gcd(k,n)=1} \left(t + e^{\frac{2\pi i k}{n}}\right) \underset{(\star)}{=} \prod_{\gcd(k,n)=1} \left(-t - e^{\frac{2\pi i k}{n}}\right) = \Phi_n(-t)$$

נצדיק את המעבר של $(\star)$ ובזה נסיים: אנחנו יודעים שפולינום ציקלוטומי מסדר n הוא יחיד ושהמקדם המוביל שלו הוא 1 ודרגתו היא $\varphi_{\text{אויילר}}(n)$ אז עבור ξ שורש יחידה פרימיטיבי כלשהו מסדר n מתקיים

$$\left(-t - \xi^k\right) = -\left(t + \xi^k\right) = (-1)^{\varphi_{\text{אויילר}}(n)}\left(x + \xi^k\right)$$

ומיחידות הפולינום הציקלוטומי (בגלל המקדם המוביל), ניתן להשמיט את הסימן. $\square$

תת־סעיף ב'

אם p ראשוני אז $\Phi_{pn}(t) = \Phi_n(t^p)$ אם $p \mid n$ ואחרת $\Phi_{pn}(t) = \frac{\Phi_n(t^p)}{\Phi_n(t)}$.

הוכחה: יהי p ראשוני ו־$n \in \mathbb{N}$, באינדוקציה על n נראה שמתקיים

$$\Phi_{pn}(t) = \begin{cases} \Phi_n(t^p) & p \mid n \\ \frac{\Phi_n(t^p)}{\Phi_n(t)} & p \nmid n \end{cases}$$

וראינו שעבור p ראשוני מתקיים

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

וההגדרה של פולינום ציקלוטומי

$$t^n - 1 = \prod_{d \mid n} \Phi_d(t) \Rightarrow t^{pn} - 1 = \prod_{d \mid pn} \Phi_d(t)$$

נתתחיל מלהראות עבור $p \nmid n$ ונשתמש בהגדרה האינדוקטיבית שראינו ל־Φ_n

$$\Phi_n(t) = \frac{t^p - 1}{\prod_{d \mid n, d \neq n} \Phi_d}$$

ואכן, עבור $n = 1$ מתקיים

$$\Phi_p(t) = \frac{t^p - 1}{\prod_{d \mid 1, d \neq 1} \Phi_d} = \frac{t^p - 1}{\Phi_1(t)} = \frac{\Phi_1(t^p)}{\Phi_1(t)}$$

נניח שהטענה נכונה עבור $n \in \mathbb{N}$ כך ש־$n \nmid p$ ומתקיים

$$\Phi_{pn}(t) = \frac{\Phi_n(t^p)}{\Phi_n(t)}$$

ונחשב

$$\Phi_{pn}(t) = \frac{t^{pn}-1}{\prod_{\substack{d|pn \\ d\neq pn}} \Phi_d(t)} = \frac{t^{pn}-1}{\Phi_n(t)\cdot\prod_{\substack{d|n \\ d\neq n}} \Phi_{pd}(t)\cdot\prod_{\substack{d|n \\ d\neq n}} \Phi_d(t)} \underset{\text{הנחת האינדוקציה}}{=} \frac{1}{\Phi_n(t)}\cdot\frac{t^{pn}-1}{\prod_{\substack{p|n \\ p\neq n}} \frac{\Phi_d(t^p)}{\Phi_d(t)}}\cdot\frac{1}{\prod_{\substack{d|n \\ d\neq n}} \Phi_d(t)}$$

$$= \frac{(t^p)^n-1}{\prod_{\substack{p|n \\ p\neq n}} \Phi_d(t^p)}\cdot\frac{1}{\Phi_n(t)} = \frac{\frac{\Phi_n(t^p)}{\Phi_n(t)}}{\prod_{\substack{p|n \\ p\neq n}} \Phi_d(t^p)}\cdot\frac{1}{\Phi_n(t)} = \frac{\Phi_n(t^p)}{\Phi_n(t)}$$

ניתן היה להפעיל את הנחת האינדוקציה כי אם $n \nmid p$ אז $d \nmid p$.

נראה כעת עבור המקרה בו $p \mid n$ ולכן $n = p^\ell k$ עבור $k \nmid p$ ונצטרך לעשות אינדוקציה על ℓ.

עבור בסיס האינדוקציה (יש פה אינדוקציה בתוך אינדוקציה), נניח ש־$\ell = 1$ ולכן $n = pk$, נחלק לשני מקרים

1. $k = 1$ ולכן $n = p$ ובמקרה זה מתקיים מצד אחד

$$\Phi_{pp}(t) = \Phi_{p^2}(t) = t^{p^2}-1$$

ומצד שני

$$\Phi_{pp}(t) = \Phi_{p^2}(t) = \prod_{d|p^2}\Phi_d(t) = \Phi_1(t)\Phi_p(t)\Phi_{p^2}(t)$$

ולכן

$$\Phi_{p^2}(t) = \frac{t^{p^2}-1}{\Phi_1(t)\Phi_p(t)} = \frac{t^{p^2}-1}{(t-1)\left(\frac{t^p-1}{t-1}\right)} = \frac{t^{p^2}-1}{t^p-1}$$

אבל

$$\Phi_p(t^p) = \frac{t^{p^p}-1}{t^p-1} = \frac{t^{p^2}-1}{t^p-1}$$

וזה סוגר את המקרה הזה.

2. לכל $k \mid d$ נסמן $n' = pd$ מתקיים $\Phi_{pn'}(t) = \Phi_{n'}(t^p)$ ואז

$$\Phi_{p^2k}(t) = \frac{t^{p^2k}-1}{\prod_{\substack{d|p^2k \\ d\neq p^2k}} \Phi_d(t)} = \frac{t^{p^2k}-1}{\prod_{d|k}\Phi_d(t)\prod_{\substack{d|k \\ p\nmid d}}\Phi_p^d(t)\prod_{\substack{d|k \\ d\neq k}}\Phi_{p^2d}(t)} \underset{p\nmid d}{=} \frac{(t^p)^{pk}-1}{\prod_{d|k}\Phi_d(t)\prod_{d|k}\left(\frac{\Phi_d(t^p)}{\Phi_d(t)}\right)\prod_{\substack{d|k \\ d\neq k}}\Phi_{p^2d}(t)}$$

$$\underset{\text{הנחת האינדוקציה } p|k}{=} \frac{(t^p)^{pk}-1}{\prod_{d|k}\Phi_d(t^p)\prod_{\substack{d|k \\ d\neq k}}\Phi_{pd}(t^p)} = \frac{(t^p)^{pk}-1}{\prod_{\substack{d|pk \\ d\neq pk}}\Phi_d(t^p)} = \Phi_{pk}(t^p)$$

נניח עכשיו שהטענה נכונה לכל $1 \leq \ell' < \ell$ ונראה שהטענה נכונה עבור ℓ, אז נסמן $n' = p^{\ell'}d$ שמתקיים $\Phi_{pn'}(t) = \Phi_{n'}(t^p)$ ואז

$$\Phi_{pn}(t) = \frac{t^{pn}-1}{\prod_{\substack{d|pn \\ d\neq pn}}\Phi_d(t)} = \frac{t^{pn}-1}{\prod_{\substack{d|p^\ell k \\ d\neq p^\ell k}}\Phi_d(t)} = \frac{(t^p)^n-1}{\prod_{d|k}\Phi_d(t)\prod_{d|k}\Phi_{pd}(t)}\prod_{\substack{d|k \\ 1\leq\ell'<\ell}}\Phi_{pp^{\ell'}d}(t^p))$$

$$\underset{\text{הנחת האינדוקציה}}{=} \frac{(t^p)^n-1}{\prod_{d|k}\Phi_d(t)\prod_{d|k}\Phi_{pd}(t)\prod_{\substack{d|k \\ 1\leq\ell'<\ell}}\Phi_{p^{\ell'}d}(t^p)} \underset{(\star)}{=} \frac{(t^p)^n-1}{\prod_{\substack{d|n \\ p\nmid d}}\Phi_d(t^p)\prod_{\substack{d|p^\ell k=n \\ p|d \\ d\neq p^\ell k}}\Phi_d(t^p)} = \frac{(t^p)^n-1}{\prod_{\substack{d|n \\ d\neq n}}\Phi_d(t^p)} = \Phi_n(t^p)$$

היה ניתן להשתמש בהנחת האינדוקציה כי $n' = p^{\ell'}k$ ו־$(\star)$ נובע מכך ש־$d \nmid p$ ולכן $\Phi_{pd}(t) = \frac{\Phi_d(t^p)}{\Phi_d(t)}$. □

סעיף ב'

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

פתרון: ראינו שפולינום ציקלוטומי מסדר n נתון על־ידי

$$\Phi_n = \prod_{\omega \text{ שורש יחידה מסדר } n} (x-\omega)$$

אז

$$\Phi_1 = x-1, \Phi_2 = x+1$$

שכן 1 הוא המספר המורכב היחידי מסדר 1 ו־(-1) הוא המספר המרוכב היחידי מסדר 2.
באותו אופן, בגלל ש־$\{\pm i\}$ הם המרוכבים היחידים מסדר 4, כבר אפשר לנחש שמתקיים

$$\Phi_4 = (x-i)(x+i) = x^2+1$$

נחשב גם את Φ_3 באותה דרך, אנחנו יודעים ש־$\omega = -\frac{1}{2} + \left(i\frac{\sqrt{3}}{2}\right)$ ואז $\{\omega, \omega^2\}$ הם שורשי יחידה פרימיטיביים מסדר 3 ולכן

$$\Phi_3 = (x-\omega)(x-\omega^2) = x^2 - x\omega^2 - x\omega + \omega^3 = x^2 - x\left(-\frac{1}{2}+\frac{i\sqrt{3}}{2}\right)^2 - x\left(-\frac{1}{2}+\frac{i\sqrt{3}}{2}\right) + 1$$

$$= x^2 - x\left(-\cancel{\frac{i\sqrt{3}}{2}} - \frac{1}{2}\right) - x\left(-\frac{1}{2} + \cancel{\frac{i\sqrt{3}}{2}}\right) + 1 = x^2+x+1$$

ניזכר שראינו במטלה 3 שעבור p ראשוני ו־$n \in \mathbb{N}$, הפולינום הציקלוטומי מסדר p^n הוא $\frac{x^{p^n}-1}{x^{p^{n-1}}-1}$. נשתמש בזה עבור $p = 5, 7$ עם $n = 1$ ונקבל

$$\Phi_5 = \frac{x^{5^1}-1}{x^{5^{1-1}}-1} = \frac{x^5-1}{x-1} = \frac{(x-1)(x^4+x^3+x^2+x+1)}{x-1} = x^4+x^3+x^2+x+1$$

$$\Phi_7 = \frac{x^{7^1}-1}{x^{7^{1-1}}-1} = \frac{x^7-1}{x-1} = \frac{(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)}{x-1} = x^6+x^5+x^4+x^3+x^2+x+1$$

את Φ_6 נחשב עם סעיף א' תת־סעיף א' ונקבל

$$\Phi_6 = \Phi_{2\cdot 3}(t) = \Phi_3(-t) = x^2-x+1$$

ובאותו אופן אפשר גם את Φ_{10}

$$\Phi_{10} = \Phi(2\cdot 5)(t) = \Phi_5(-t) = x^4-x^3+x^2-x+1$$

עבור Φ_9, נשתמש עם סעיף א' תת־סעיף ב' עבור $p = n = 3$ ונקבל

$$\Phi_9 = \Phi_{3\cdot 3}(t) = \Phi_3(t^3) = x^6+x^3+1$$

אחרון חביב נשאר לחשב את Φ_8 ובאותו אופן ל־Φ_9 נבחר $p = 2, n = 4$ ונקבל

$$\Phi_8 = \Phi_{2\cdot 4} = \Phi_2(t^4) = x^4+1$$

את אלו שנשארו, נחשב עם נשאר לחשב עבור $5 \leq n \leq 10$: מפונקציית $\varphi_{\text{אויילר}(5)} = 5-1 = 4$ ולכן יש לנו ארבעה שורשי יחידה מסדר 5
בסך־הכל קיבלנו

$$\Phi_1 = x-1, \Phi_2 = x+1, \Phi_3 = x^2+x+1, \Phi_4 = x^2+1, \Phi_5 = x^4+x^3+x^2+x+1$$

$$\Phi_6 = x^2-x+1, \Phi_7 = x^6+x^5+x^4+x^3+x^2+x+1, \Phi_8 = x^4+1, \Phi_9 = x^6+x^3+1, \Phi_{10} = x^4-x^3+x^2-x+1$$

□

שאלה 3

בהרצאה ראינו ש־$\mathbb{F}_{p^d}/\mathbb{F}_p$ היא הרחבה ציקלוטומית על־ידי שורש יחידה ξ מסדר p^d-1 ושבמצב כזה קיים שיכון

$$\mathrm{Aut}\big(\mathbb{F}_{p^d}/\mathbb{F}_p\big) \hookrightarrow \mathrm{Aut}\big(\mu_{p^d-1}\big) \xrightarrow{\sim} \big(\mathbb{Z}/(p^d-1)\mathbb{Z}\big)^\times$$

נתאר את השיכון $\mathrm{Aut}_{\mathbb{F}_p}\left(\mathbb{F}_{p^d}\right) = \mathrm{Fr}_p^{\mathbb{Z}/d\mathbb{Z}} \hookrightarrow \big(\mathbb{Z}/(p^d-1)\mathbb{Z}\big)^\times$ ונקבע את תמונת איבר הפרובניוס Fr_p.

הוכחה: אנחנו יודעים ש־$\mathbb{F}_{p^d}^\times$ היא חבורה ציקלית ולכן נסמן $\mathbb{F}_{p^d}^\times = \langle\xi\rangle$ עבור $\xi \in \mathbb{F}_{p^d}$ וכל $0 \neq \alpha \in \mathbb{F}_{p^d}^\times$ הוא מהצורה ξ^k עם $k \in \mathbb{Z}/\big(p^d-1\big)\mathbb{Z}$ וכבר ראינו בהרצאה ובתרגיל הקודם ש־$\big(\mathbb{Z}/(p^d-1)\mathbb{Z}\big) \simeq \mathbb{F}_{p^d}^\times = \mu_{p^d-1}$ באמצעות exp.

מכיון שהשדה סופי, אנחנו יודעים שהפרובניוס הוא אוטומורפיזם (למה? אנחנו יודעים שפרובניוס הוא הומומורפיזם, והוא חד־חד ערכי כי אם $\mathrm{Fr}_p(x) = \mathrm{Fr}_p(y)$ אז $x^p = y^p$ ובגלל שאין מחלקי אפס כי זה תחום שלמות קיבלנו חד־חד ערכיות. וכל העתקה חד־חד ערכית מקבוצה אל עצמה היא על ולכן אוטומורפיזם) ולכן

$$\mathrm{Aut}_{\mathbb{F}_p}\left(\mathbb{F}_{p^d}\right) = \left\{\mathrm{Fr}_p^k : x \mapsto x^{p^k} \mid k \in [d-1]\right\}$$

היא חבורה ציקלית מסדר d (כי $x^{p^d} = x$ לכל x ואין חזקה נמוכה יותר שעושה את זה).
ניקח את ξ ממקודם, ומתקיים $\mathrm{Fr}_p^{k(\xi)} = \xi^{p^k}$ ולכן לכל $k \in [d-1]$ נקבל

$$\mathrm{Fr}_p^k : \xi^m \mapsto (\xi^m)^{p^k} = \xi^{m\cdot p^k}$$

שזו בעצם מכפלה ב־$p^k \bmod \big(p^d-1\big)$ וזה בעצם אוטומורפיזם כפלי של החבורה הציקלית μ_{p^d-1}.
בגלל שאוטומורפיזם מכבד את מבנה החבורה נקבל $\mathrm{Fr}_p^k \in \mathrm{Aut}_{\mathbb{F}_p}\left(\mathbb{F}_{p^d}\right)$

$$\mathrm{Fr}_p^k \mapsto [p^k] \in \big(\mathbb{Z}/(p^d-1)\mathbb{Z}\big)^\times$$

□

שאלה 4

תהיי $q = p^k$ 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 $\mathbb{F}_q$ ולפולינום אי־פריק מדרגה $d > 1$ מעל $\mathbb{F}_q$ שאינו פרימיטיבי.

פתרון: נבחר $k = 1, p = 3$ והפולינום $f(x) = x^2 + 1$ הוא אי־פריק ב־$\mathbb{F}_3$ כי אין לו שורשים ולכן לפי מטלה 1 הוא אי־פריק, ו־$\deg(f)_{\mathbb{F}_3} = 2$.

בהרצאה ראינו תרגיל שמתקיים $\mathbb{F}_9 = \mathbb{F}_3(i)$ (זה נובע מכך של־$f(x)$ אין שורשים ב־$\mathbb{F}_3$, וכל איבר ב־$\mathbb{F}_3(i)$ הוא מהצורה $a + bi \in \mathbb{F}_3$ ו־$i^2 = 2$

ולכן יש לנו 9 צירופים אפשריים מקומבינטוריקה, וממשפט שראינו בהרצאה שלכל ראשוני $p \in \mathbb{N}$ ו־$q = p^n$ עבור $n \geq 1$ קיים שדה $\mathbb{F}_q$ עם q איברים והוא יחיד עד־כדי איזומורפיזם). אבל $0 = 1 + 2 = f\left(\sqrt{2}\right)$ הוא שורש של $f(x)$ מעל $\mathbb{F}_3\left(\sqrt{2}\right)$ ומהמשפט שהזכרנו נובע ש־$\mathbb{F}_9 \simeq$ $\mathbb{F}_3\left(\sqrt{2}\right)$.

אבל גם מתקיים $\left|\mathbb{F}_{q^d}^\times\right| = 3^2 - 1 = 8$ ו־$\left(\sqrt{2}\right)^4 = 4 = 1 \in \mathbb{F}_3\left(\sqrt{2}\right)$ ולכן $o\left(\sqrt{2}\right) \leq 4 < 8$ ולכן לא ייתכן ש־$\sqrt{2}$ ייצור את $\mathbb{F}_{q^d}^\times$.

זה עונה על תנאי השאלה. □

סעיף ב'

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

הוכחה: יהי $\alpha \in \mathbb{F}_{q^d}$ יוצר של $\mathbb{F}_{q^d}^\times$. אז המסלול שלו ב־$\mathrm{Aut}\left(\mathbb{F}_{q^d}/\mathbb{F}_q\right)$ זה קבוצת הצמודים שלו, C_α, אז

$$|o(\alpha)| = |C_\alpha| = \left|\deg(f)_{\alpha/\mathbb{F}_q}\right| = \left[\mathbb{F}_q(\alpha) : \mathbb{F}_q\right]$$

אבל α הוא יוצר של $\mathbb{F}_{q^d}^\times$ ולכן

$$\left[\mathbb{F}_q(\alpha) : \mathbb{F}_q\right] = \left[\mathbb{F}_{q^d} : \mathbb{F}_q\right] = d$$

□

סעיף ג'

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

הוכחה: ראינו ש־$\mathbb{F}_{q^d}^\times$ היא חבורה ציקלית מסדר $q^d - 1$ ולכן מספר היוצרים שלה הוא $\varphi\left(q^d - 1\right)$, נסמן $A = \left\{\alpha \in \mathbb{F}_{q^d}^\times \mid \langle\alpha\rangle = \mathbb{F}_{q^d}^\times\right\}$, קבוצת היוצרים.

כל פולינום אי־פריק $f \in \mathbb{F}_q[x]$ מדרגה d יש לו d שורשים ב־$\mathbb{F}_{q^d}[x]$ אשר צמודים תחת הפרובניוס

$$\left\{\alpha, \alpha^q, \alpha^{q^d}, ..., \alpha^{q^{d-1}}\right\}$$

עם המיפוי $\sigma : x \mapsto x^q$ (פורבניוס אוטומורפיזם ב־$\mathbb{F}_q$).

יהי $\alpha \in A$ הפולינום המינימלי המתוקן מעל $\mathbb{F}_q[x]$ עם α בתור שורש הוא $f_\alpha(x)$, אבל גם כל הצמדת פרבוניוס α לעיל היא גם שורש של הפולינום המינימלי הזה, וזה אומר שכל המסלול של ההצמדה לעיל הם שורשים של $f_\alpha(x)$, משמע יש d שורשים: כל מסלול ההצמדה.

ברור שלכל פרימיטיבי אין את אותו המסלול כי יש לכל אחד מהם מסלול שונה תחת הצמדת הפרובניוס ולכן כל פולינום פרימיטיבי מגיע ממסלול אחד בגודל d.

אז ראינו שכל הפרימיטיביים הם בידיוק $\varphi\left(q^d - 1\right)$ (זה גם בעצם $|A|$), כל מחלקת צמידות כזאת מתחלקת למסלולים שונים מגודל d ולכן מספר המסלולים האלו, שכפי שראינו עכשיו זה מספר הפולינומים הפרימיטיביים זה בידיוק $\frac{\varphi(q^d-1)}{d}$.

□