פתרון מטלה 06 — מבנים אלגבריים 2, 80446

23 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

$$2 \mid (2k+n) \Rightarrow 2k + n \equiv 0 (\bmod 2) \Rightarrow n \equiv -2k \equiv 0 (\bmod 2) \Rightarrow n \equiv 0 (\bmod 2) \Rightarrow 2 \mid n$$

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. □

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: TODOOOOOOOOOOOOOOOOOOO 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

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

נתחיל 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

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

ונראה שהטענה נכונה גם עבור $m>n$ כך ש־$p\nmid m$ אז לפי הגדרה, מתקיים

$$t^{pn'}-1=\prod_{d|pn'}\Phi_d(t)$$

נסתכל על המחלקים של pn':

1. אם $p\mid d$ אז $d=pk$ ולכן $k\mid n'$
2. אם $p\nmid d$ אז $d\mid n'$

ולכן נקבל

$$t^{pn'}-1=\prod_{d|pn'}\Phi_d(t)=\prod_{d|pn',p|d}\Phi_d(t)\cdot\prod_{d|pn',p\nmid d}\Phi_d(t)$$

אבל גם מתקיים

$$t^{pn'}-1=\left(t^{n'}\right)^p-1=\prod_{d|n'}\Phi_d(t^p)$$

(ראינו את זה כבר במטלה קודמת / בהרצאה, זה הטריק של $t\mapsto t^p$).
אז יש לנו בסך־הכל

$$\prod_{d|pn',p|d}\Phi_d(t)\cdot\prod_{d|pn',p\nmid d}\Phi_d(t)=\prod_{d|n'}\Phi_d(t^p)$$

$\square$

סעיף ב'

נחשב את $\Phi_n(t)$ לכל $1\le n\le 10$.
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 $5 \le n \le 10$: מפונקציית $\varphi_{\text{אויילר}}(5) = 5 - 1 = 4$ ולכן יש לנו ארבעה שורשי יחידה מסדר 5 בסך־הכל קיבלנו

$$\Phi_1 = x - 1, \Phi_2 = x + 1, \Phi_3 = x^2 + x + 1, \Phi_4 = x^2 + 1, \Phi_5 = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6 = x^2 - x + 1, \Phi_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \Phi_8 = x^4 + 1, \Phi_9 = x^6 + x^3 + 1, \Phi_{10} = x^4 - x^3 + x^2 - x + 1$$

$\square$

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

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

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

הוכחה: TODOOOOOOOOOOOOOOOOOO $\square$

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 $p=3$ $k=1,$ 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 $f\left(\sqrt{2}\right)=2+1=0$ 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־$\operatorname{Aut}\left(\mathbb{F}_{p^d}/\mathbb{F}_q\right)$ מכיל d איברים שונים.
הוכחה: TODOOOOOOOOOOOOOOOOOOO □

סעיף ג'

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

שאלה 5

סעיף א'

נוכיח שמתקיים

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{k|d} f(k) = \sum_{k|n} f(k) \sum_{m|(n/k)} \mu\left(\frac{n}{km}\right)$$

הוכחה: TODOOOOOOOOOOOOOOOOOOO $\square$

סעיף ב'

נעזר בסעיף הקודם ונראה שמתקיים

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{k|n} f(k) \sum_{m|(n/k)} \mu(m)$$

הוכחה: TODOOOOOOOOOOOOOOOOOOO $\square$

סעיף ג'

נוכיח שלכל $n > 1$ מתקיים $\sum_{d|n} \mu(d) = 0$ ונסיק שמתקיים

$$\sum_{k|n} f(k) \sum_{m|(n/k)} \mu(m) = f(n)$$

הוכחה: TODOOOOOOOOOOOOOOOOOOO $\square$