פתרון מטלה 07 — מבנים אלגבריים 2, 80446

30 במאי 2025

שאלה 1

שאלה 2

תהיי $L/\mathbb{Q}$ הרחבה אלגברית נוצרת סופית. נוכיח שב־L יש מספר סופי של שורשי יחידה.

הוכחה: נניח בשלילה שב־L יש מספר לא סופי של שורשי יחידה, משמע $\{\xi_n\}_{n=1}^{\infty}$ היא סדרת שורשי יחידה שונים זה מזה כך שלכל $n \in \mathbb{N}$ מתקיים ש־ $\xi_n \in \{\xi_n\}_{n=1}^{\infty}$ הוא שורש יחידה פרימיטיבי מסדר n ו־$\xi_n \in L$.

בהרצאה ראינו ששורש היחידה ה־n־י מוכל בהרחבה הציקלוטומית $\mathbb{Q}(\xi_n)$ וראינו גם שהדרגה של ההרחבה $\mathbb{Q}(\xi_n)/\mathbb{Q}$ נתונה לפי $\varphi_{\text{אויילר}}(n)$, ולכן $[\mathbb{Q}(\xi_n):\mathbb{Q}] = \varphi_{\text{אויילר}}(n)$ והרחבה זו היא הרחבה סופית.

אם L מכילה אינסוף שורשי יחידה שונים זה מזה, היא מכילה גם אינסוף הרחבות ציקלוטומיות $\mathbb{Q}(\xi_n)$, ומכך שלכל $n \in \mathbb{N}$ מתקיים $\varphi_{\text{אויילר}}(n) > 0$, ו־$L$ מכילה את כל ההרחבות הנ"ל דרגתה מעל $\mathbb{Q}$ חייבת להכיל לכל הפחות את כל הדרגות של השדות הציקלוטומיים ולכן

$$[L:\mathbb{Q}] \geq \sum_{n=1}^{\infty} \varphi_{\text{אויילר}}(n)$$

אבל $\sum_{n=1}^{\infty} \varphi_{\text{אויילר}}(n)$ הוא סכום מתבדר כסכום אינסופי של מספרים חיוביים, ולכן $[L:\mathbb{Q}] = \infty$, אבל L היא הרחבה סופית ולכן $[L:\mathbb{Q}] < \infty$ וזאת סתירה. $\square$

שאלה 3

יהי K שדה הפיצול של $f(x) = x^8 - 2$ מעל $\mathbb{Q}$.

סעיף א'

נוכיח שניתן לזהות את K עם השדה $\mathbb{Q}(i)\left(\sqrt[8]{2}\right) \subset \mathbb{C}$ כאשר $\sqrt[8]{2}$ ממשי חיובי.

הוכחה: נשים לב שכל שורשי f הם

$$\left\{\sqrt[8]{2}e^{\frac{k\pi i}{4}} \mid 0 \leq k \leq 7\right\}$$

ניזכר ששדה פיצול הוא תת־השדה המינימלי של $\mathbb{C}$ שמכיל את שורשי f, ולכן על שדה הפיצול להכין את $\sqrt[8]{2}$ ואת ξ_8 שורש יחידה פרימיטיבי מסדר 8, כאשר

$$\xi_8 = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}} = \cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}}(1+i)$$

ולכן $\xi_8 \in \mathbb{Q}\left(i, \sqrt{2}\right)$ ולכן נסיק ש־$\mathbb{Q}(\xi_8) \subseteq \mathbb{Q}\left(i, \sqrt{2}\right)$.

נטען כעת ש־$\sqrt{2} \in \mathbb{Q}\left(\sqrt[8]{2}\right)$, כי אם נסמן $\alpha = \sqrt[8]{2}$ אז $\alpha^8 = 2$ ואז $\alpha^4 = \sqrt{2}$ ולכן $\sqrt{2} \in \mathbb{Q}\left(\sqrt[8]{2}\right)$, ולכן $\xi_8 \in \mathbb{Q}\left(i, \sqrt[8]{2}\right)$ הוספנו רק את השורשים המינימליים עלינו להוסיף משמע $\mathbb{Q}\left(i, \sqrt[8]{2}\right)$ הוא שדה הפיצול של הפולינום f ולכן ניתן לזהות את K עם השדה $\mathbb{Q}(i)\left(\sqrt[8]{2}\right)$. $\square$

סעיף ב'

נראה ש־$x^8 - 2$ אי־פריק ב־$\mathbb{Q}(i)$.

הוכחה: ראשית, $x^8 - 8$ הוא פולינום אי־פריק מעל $\mathbb{Q}[x]$ מקריטריון אייזנשטיין: נבחר $p = 2$ ואכן $a_n = 1 \nmid 2$, $2 \mid 2$ ו־$2 \nmid 2^2$ ולכן זה פולינום אי־פריק ב־$\mathbb{Q}[x]$ (כל המקדים שלמים ולכן ניתן להשתמש בקריטריון אייזנשטיין).

נניח בשלילה ש־$x^8 - 2$ הוא פולינום פריק ב־$\mathbb{Q}(i)$ ולכן קיימים $f, g \in \mathbb{Q}(i)[x]$ כך שמתקיים

$$x^8 - 2 = f(x)g(x)$$

היות ו־$\deg(x^8 - 2) = 8$ אז $\deg(f) + \deg(g) = 8$, וזה נותן לנו את הצמדים הבאים כאפשרויות:

1. $\deg(f) = 1, \deg(g) = 7$
2. $\deg(f) = 2, \deg(g) = 6$
3. $\deg(f) = 3, \deg(g) = 5$
4. $\deg(f) = 4, \deg(g) = 4$

את הפירוק $\deg(f) = \deg(4) = 4$ קל לפסול, שכן והאופציה היחידה היא $f(x) = x^4 - \sqrt{2}, g(x) = x^4 + \sqrt{2}$ אבל $f(x), g(x) \notin \mathbb{Q}(i)[x]$ כי $\sqrt{2} \notin \mathbb{Q}(i)$.

נשים לב שכל שורשי $x^8 - 2$ הם

$$\left\{\sqrt[8]{2}\frac{e^{k\pi i}}{4} \mid 0 \leq k \leq 7\right\}$$

גם עבור המקרה של $\deg(f) = 1, \deg(g) = 7$ נקבל סתירה: $\deg(f) = 1$ אומר ש־$f(x) = x - r \in \mathbb{Q}(i)$, משמע $f(x) = a + bi$.

אם $x^8 - 2$ מתפרק לגורמים שאחד מהם לינארי זה אומר ש־r הוא שורש שלו, אבל $\sqrt[8]{2} \notin \mathbb{Q}(i)$ כי $\sqrt[8]{2} \in \mathbb{R}$ ולכן גם מכפלה שלו ב־$\frac{e^{k\pi i}}{4}$ עבור $0 \leq k \leq 7$ תוביל לנו לכך שיש לנו עדיין גורם ממשי ולכן גם מקרה זה לא אפשרי.

נבחין שגם שתי הקומבינציות האחרות יפלו על אותו הדבר ולכן $x^8 - 2$ הוא פולינום אי־פריק מעל $\mathbb{Q}(i)$. $\square$

סעיף ג'

נוכיח שעבור $\varepsilon \in \{1, -1\}$ ולכל שורש z של $x^8 - 2$ קיים אוטומורפיזם של K ששולח את i ל־εi ואת $\sqrt[8]{2}$ ל־z.

הוכחה: נגדיר $\sigma : K \to K$ על־ידי $\sigma(i) = \varepsilon i, \sigma\left(\sqrt[8]{2}\right) = z = \sqrt[8]{2} \cdot \xi_8^k$ ונראה שזה מגדיר אוטומורפיזם.

ראשית, $i \in K$ הוא שורש של הפולינום $x^2 + 1$ אז גם εi הוא שורש של $x^2 + 1$ ולכן השורש הזה נשמר.

$\sqrt[8]{2}$ הוא שורש של הפולינום $x^8 - 2$ וראינו כבר שכל השורשים שלו (שאלו בעצם הצמודים שלו) הם מהצורה $\sqrt[8]{2} \cdot \xi_8^k \in K$ ולכן המיפוי $\sqrt[8]{2} \mapsto \sqrt[8]{2} \cdot \xi_8^k$ משמע שורש יחידה נשלח לשורש יחידה ולכן המיפוי הזה מוגדר היטב.

נשים לב שגם מתקיים

$$\sigma(i)^2 = (\varepsilon i)^2 = -1 = i^2$$

$$\sigma\left(\sqrt[8]{2}\right)^8 = \left(\sqrt[8]{2} \cdot \xi_8^k\right)^8 = 2 \cdot \xi_8^{8k} = 2 \cdot 1 = 2 = \left(\sqrt[8]{2}\right)^8$$

משמע, הפולינום המינימלי של שני הפולינומים לעיל נשמר, ולכן זה הומומורפיזם כי הוא מעביר יוצרים אל שורשים מתאימים אחרים של הפולינומים המינימליים שראינו לעיל.

אז זה הומומורפיזם של שדות ולכן הוא חד־חד ערכי ומטעמי סדר נקבל שהוא על ולכן σ איזומורפיזם בין שדה לבין עצמו ולכן אוטומורפיזם. $\square$

סעיף ד'

נמצא שיכון של $\mathrm{Aut}(K/\mathbb{Q})$ אל תוך החבורה המתוארת בשאלה 1 ונכתוב את התמונה.

הוכחה: ניקח את האוטומורפיזם שמצאנו בסעיף הקודם, ואז

$$\sigma\left(e^{\frac{\pi i}{4}}\right) = \frac{1 + \sigma(i)}{\sigma\left(\sqrt{2}\right)} = \frac{1 + \varepsilon i}{(-1)^k \sqrt{2}} = e^{\frac{\pi i}{4}(4k+\varepsilon)}$$

ואז עם מה שמצאנו בשאלה 1 מתקיים $\phi(\sigma) = (c, k)$ ונקבל $c \in \{4k-1, 4k+1\}$ ואז

$$\mathrm{Im}(f) = \{(c, k) \mid k \in \mathbb{Z}_8 mc \in \{4k-1, 4k+1\}\} = \left\{(c, k) \,\middle|\, k \in \mathbb{Z}_8, c \in \begin{cases} \{1{,}7\} & 2 \mid k \\ \{3{,}5\} & 2 \nmid k \end{cases}\right\}$$

TODOOOOOOOOOOOOOOOOOO $\square$

סעיף ה'

נקבע האם החבורה משאלה 1 היא אבלית והאם היא חבורה דיהדרלית.

הוכחה: **TODOOOOOOOOOOOOOOOOOO** היא לא חבורה אבלית, שכן $(1, 2) \cdot (3, 3) = (3, 5) \neq (3, 1) = (3, 3) \cdot (1, 2)$ $\square$

שאלה 4

יהי p ראשוני ונסמן $K=\overline{\mathbb{F}_p}(s,t)$.

סעיף א'

נוכיח ש־$\left[K^{\frac{1}{p}}:K\right]=p^2<\infty$.

הוכחה: קודם כל נשים לב ש־$s^{\frac{1}{p}}\in K^{\frac{1}{p}}$ כי $\left(s^{\frac{1}{p}}\right)^p=s\in K$ ובאותו אופן גם $t^{\frac{1}{p}}\in K^{\frac{1}{p}}$ כי $\left(t^{\frac{1}{p}}\right)^p=t\in K$ ואז $K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right)\subseteq K^{\frac{1}{p}}$.

נראה את ההכלה בכיוון השני, יהי $x\in K^{\frac{1}{p}}$ ואז $x^p\in K$ והוא מהצורה $x^p=\frac{f(s,t)}{g(s,t)}\in\overline{\mathbb{F}_p}(s,t)$.

נטען כי $\overline{\mathbb{F}_p}$ הוא פרפקט – שכן הוא סגור אלגברית והפולינומים האי־פריקים היחידים שיש הם אלו הם מדרגה 1 ולכן אין להם שורשים מרובים, אז הם ספרבילים ולכן זה פרפקט.

אם נכתוב את f,g בתור פולינומים פורמליים נקבל

$$x^p=\frac{f(s,t)}{g(s,t)}=\frac{\sum_{(i,j)}a_{i,j}s^it^j}{\sum_{(k,l)}b_{k,l}s^it^j}$$

אבל מהפרפקטיות שראינו נובע שלכל $a_{i,j},b_{k,l}\in\overline{\mathbb{F}_p}$ יש שורש מסדר p, ולכן

$$s^i=\left(s^{\frac{1}{p}}\right)^{pi},t^j=\left(t^{\frac{1}{p}}\right)^{pj},a_{i,j}=\left(a_{i,j}^{\frac{1}{p}}\right)^p$$

עבור הפולינום f ובאותו אופן גם עבור הפולינום g, אז

$$x^p=\frac{f(s,t)}{g(s,t)}=\left(\frac{\sum_{(i,j)}\left(a_{i,j}\right)^{\frac{1}{p}}s^{\frac{i}{p}}t^{\frac{j}{p}}}{\sum_{(k,l)}\left(b_{k,l}\right)^{\frac{1}{p}}s^{\frac{k}{p}}t^{\frac{l}{p}}}\right)^p$$

ולכן

$$x=\frac{\sum_{(i,j)}\left(a_{i,j}\right)^{\frac{1}{p}}s^{\frac{i}{p}}t^{\frac{j}{p}}}{\sum_{(k,l)}\left(b_{k,l}\right)^{\frac{1}{p}}s^{\frac{k}{p}}t^{\frac{l}{p}}}$$

ואז $x\in K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right)$ וקיבלנו את ההכלה בכיוון השני, משמע $K^{\frac{1}{p}}\subseteq K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right)$.

ראינו הכלה בשני הכיוונים ולכן $K^{\frac{1}{p}}=K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right)$.

נעבור לחשב את הדרגה הנדרשת ונשתמש בכפליות הדרגה

$$\left[K^{\frac{1}{p}}:K\right]=\left[K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right):K\right]=\left[K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right):K\left(s^{\frac{1}{p}}\right)\right]\cdot\left[K\left(s^{\frac{1}{p}}\right):K\right]$$

היות ו־$s^{\frac{1}{p}}\notin K$ זה שורש של הפולינום $x^p-s=0$ שאנחנו כבר יודעים שהוא פולינום אי־פריק בשדה עם מאפיין p, אז $\left[K\left(s^{\frac{1}{p}}\right):K\right]=p$, באותו אופן גם $t^{\frac{1}{p}}\notin K\left(s^{\frac{1}{p}}\right)$ היא שורש של הפולינום x^p-t שהוא שוב אי־פריק ולכן שוב הדרגה היא p ומכפליות הדרגה

$$\left[K^{\frac{1}{p}}:K\right]=\left[K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right):K\right]=\left[K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right):K\left(s^{\frac{1}{p}}\right)\right]\cdot\left[K\left(s^{\frac{1}{p}}\right):K\right]=p\cdot p=p^2$$

□

סעיף ב'

נוכיח שלכל $\alpha,\beta\in\overline{\mathbb{F}_p}$ שונים ההרחבות $K\left(s^{\frac{1}{p}}+\alpha t^{\frac{1}{p}}\right)$ ו־$K\left(s^{\frac{1}{p}}+\beta t^{\frac{1}{p}}\right)$ שונות זו מזה ובעלות דרגה p. נסיק שיש אינסוף שדות ביניים בין K לבין $K^{\frac{1}{p}}$.

הוכחה: ניקח $x=s^{\frac{1}{p}}+\alpha t^{\frac{1}{p}}\in K^{\frac{1}{p}}$ ולכן $x^p=s+\alpha^pt\in K$ ולכן $X^p-(s+\alpha^pt)=0$ הוא פולינום אי־פריק מעל K כי הוא אי־פריד (כי הנגזרת היא 0 במציין p) ו־x הוא שורש ו־$s+\alpha^pt\notin K^p$: כי אם הוא היה, אז היה מתקיים

$$s+\alpha^pt=\left(\frac{f(s,t)}{g(s,t)}\right)^p\iff\frac{f^{p(s,t)}}{g^{p(s,t)}}=s+\alpha^pt\iff f^{p(s,t)}=g^{p(s,t)}(s+\alpha^pt)$$

אבל בצד ימין הדרגה של s,t היא 1 ובשמאל הדרגה של s,t היא מדרגה שמחלקת את p וגם אם g קבועה עדיין מטעמי דרגות אין לנו דרגת p, ולכן $s+\alpha^t p\notin K^p$ ולכן הפולינום הוא אי־פריק ואז

$$[K(x):K]=p$$

וזה סוגר את החלק הראשון, עבור החלק השני נניח בשלילה ש־$K\left(s^{\frac{1}{p}}+\alpha t^{\frac{1}{p}}\right)=K\left(s^{\frac{1}{p}}+\beta t^{\frac{1}{p}}\right)$ עבור $\beta\neq\alpha$ אז נגדיר

$$x=s^{\frac{1}{p}}+\alpha t^{\frac{1}{p}},\ y=s^{\frac{1}{p}}+\beta t^{\frac{1}{p}}$$

ולכן

$$x-y=(\alpha-\beta)t^{\frac{1}{p}}\iff\frac{x-y}{\alpha-\beta}=t^{\frac{1}{p}}\in K(x-y)$$

שמוגדר היטב כי $\beta\neq\alpha$, ולכן $t^{\frac{1}{p}}\in K(y)$ ולכן $t\in K(y)^p$ משמע $t\in K$, אבל אז

$$K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right)\subseteq K(y)$$

ובגלל יחס דרגות והכלה נקבל עם מה שמצאנו בשלב הקודם והסעיף הקודם

$$\left[K\left(s^{\frac{1}{p}},t^{\frac{1}{p}}\right):K\right]=p^2\leq p=[K(y):K]$$

אבל זו סתירה.

עבור ההסקה, $\overline{\mathbb{F}_p}$ אינסופי (כי הוא מכיל כל הרכבה אלגברית של $\mathbb{F}_p$), יש לנו אינסוף ערכים יונקיים עבור α ולכן יש אינסוף שדות $K\left(s^{\frac{1}{p}}+\alpha t^{\frac{1}{p}}\right)$ שכל אחד מהם מדרגה p ששונים מכל α אחרת ולכן יש אינסוף שדות ביניים. $\square$