

פתרון מטלה 07 – מבנים אלגבריים 2, 80446

4 ביוני 2025



שאלה 1

נסמן $F = \mathbb{Q}(s)$ (שדה הפונקציות הרציונליות במשתנה s מעל \mathbb{Q}). יהי K שדה הפיצול של $x^n - s \in F[x]$ ונוכיח שמתקיים

$$\text{Aut}(K/F) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \rtimes_\theta (\mathbb{Z}/n\mathbb{Z})$$

כאשר $\theta : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ הוא האוטומורפיזם המוגדר על ידי $(\theta(k))(n) = kn$.

הוכחה: אנחנו יודעים שהשורשים של הפולינום $x^n - s$ הם $\alpha, \xi_n \alpha, \xi_n^2 \alpha, \dots, \xi_n^{n-1} \alpha$ כאשר $\alpha = \sqrt[n]{s}$ ו- ξ_n שורש יחידה פרימיטיבי מסדר n .

על-כן, שדה הפיצול מהגדרה הוא $K = F(\alpha, \xi_n)$.

היות ו- α הוא שורש של הפולינום $x^n - s$ שהוא אי-פריק מעל K אז הדרגה של $F(\alpha)$ היא מסדר n ושורש יחידה פרימיטיבי הוא אלגברי מעל \mathbb{Q} . נשאר להראות שהוא אי-פריק גם מעל \mathbb{F} : נניח בשלילה שהוא לא פריק ולכן הוא מכפלה של שתי פונקציות רציונליות עם סכום מעלות n (כל אחת מהן עם דרגה קטנה מ- n). אבל בשדה הפיצול הוא מכפלה של גורמים לינאריים, ולכן המקדם של האיבר החופשי בהכרח צריך להיות שייך ל- $\mathbb{Q}(s)$. משמע הוא מהצורה של s^k כלשהו אבל אז מחילוק פולינומים $\frac{f(s)}{g(s)} = s^k$ כאשר f, g הפונקציות של הפירוק של הפולינום אבל אז $f(s) = g(s)s^k$ וב- $f(s)$ אין חזקות של s רציונליות וזו סתירה, אז $x^n - s$ הוא אי-פריק מעל F .

נסמן $\alpha = s^{\frac{1}{n}}$ ואז הצמודים של α הם מהצורה $\{\alpha, \omega_n \alpha, \dots, \omega_n^{n-1} \alpha\}$ ואלו לא דווקא כל שורשי היחידה הפרימיטיביים מסדר n מעל K אבל הם כן מוכלים בזה.

כעת נגדיר

$$\Phi : \text{Aut}(K/F) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times \rtimes_\theta (\mathbb{Z}/n\mathbb{Z})$$

על-ידי $\Phi(\sigma) = (k, a)$ כאשר $\sigma(\xi_n) = \xi_n^k, \sigma(\alpha) = \xi_n^a \alpha$ מהגדרת האוטומורפיזם.

1. זה הומומורפיזם: ניקח $\sigma_1, \sigma_2 \in \text{Aut}(K/F)$

$$\sigma_1 \sigma_2(\xi_n) = \sigma_1(\xi_n^{k_2}) = \xi_n^{k_1 k_2}, \sigma_1 \sigma_2(\alpha) = \sigma_1(\xi_n^{a_2} \alpha) = \xi_n^{k_1 a_2} \xi_n^{a_1} = \xi_n^{a_1 + k_1 a_2} \alpha$$

נשים לב שהכל מוגדר לעיל כי מהגדרת המכפלה החצי-ישרה $\Phi(\sigma_1 \sigma_2) = (k_1 k_2, a_1 + k_1 a_2)$.

2. ראינו כבר בתרגול שזה שייכון

3. זה על: אנחנו רוצים לכל $(k, a) \in (\mathbb{Z}/n\mathbb{Z})^\times \rtimes_\theta (\mathbb{Z}/n\mathbb{Z})$ שיהיה $\sigma \in \text{Aut}(K/F)$ שמקיים את התנאים $\sigma(\xi_n) = \xi_n^k, \sigma(\alpha) = \xi_n^a \alpha$.

אז נגדיר $\sigma(\xi_n) = \xi_n^k$ כי ξ_n^k הוא עדיין שורש יחידה פרימיטיבי ולכן $\xi_n \mapsto \xi_n^k$ מגדיר אוטומורפיזם $\mathbb{Q}(\xi_n)/\mathbb{Q}$ ולכן $\mathbb{Q}(\xi_n, \alpha) \subset F$ ונגדיר $\sigma(\alpha) = \xi_n^a \alpha$ ואז

$$\sigma(\alpha)^n = (\xi_n^a \alpha)^n = \xi_n^{an} \alpha^n = \xi_n^{an} s \stackrel{\xi_n^n = s}{=} s \in K$$

ולכן זה על.

□

שאלה 2

תהי 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 מוכל בהרחבה הציקלוטומית $\mathbb{Q}(\xi_n)$ וראינו גם שהדרגה של ההרחבה $\mathbb{Q}(\xi_n)/\mathbb{Q}$ נתונה לפי $\varphi_{\text{אייילר}}(n)$, ולכן $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi_{\text{אייילר}}(n)$ 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 $\varphi_{\text{אייילר}}(n) > 0$, ו- L מכילה את כל ההרחבות הנ"ל דרגתה מעל \mathbb{Q} חייבת להכיל לכל הפחות את כל הדרגות של השדות הציקלוטומיים ולכן

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

אבל $\sum_{n=1}^{\infty} \varphi_{\text{אייילר}}(n)$ 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.

□

שאלה 3

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

סעיף א'

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

סעיף ב'

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

הוכחה: ראשית, $x^8 - 2$ הוא פולינום אי-פריק מעל $\mathbb{Q}[x]$ מקריטריון אייזנשטיין: נבחר $p = 2$ ואכן $a_n = 1$ ו- $2 \nmid a_{n-1}, \dots, a_1$ ולכן זה פולינום אי-פריק ב- $\mathbb{Q}[x]$ (כל המקדמים 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 הצמידים 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 $\deg(f) = \deg(g) = 4$ 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

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

גם עבור המקרה של $\deg(f) = 1, \deg(g) = 7$ נקבל סתירה: $\deg(f) = 1$ אומר ש- $f(x) = x - r$ ו- $r \in \mathbb{Q}(i)$, משמע $f(x) = a + bi$ עם $a, b \in \mathbb{Q}$. אבל $\sqrt[8]{2} \notin \mathbb{Q}(i)$ כי $\sqrt[8]{2} \in \mathbb{R}$ ולכן גם מכפלה שלו ב- $e^{\frac{k\pi i}{4}}$ 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 $\sigma: K \rightarrow K$ על-ידי $\sigma: \sqrt[8]{2} \cdot \xi_8^k \mapsto z = \varepsilon i \cdot \sqrt[8]{2}$ 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 $\sqrt[8]{2} \mapsto \varepsilon i \cdot \sqrt[8]{2}$ משמע שורש יחידה נשלח לשורש יחידה ולכן המיפוי הזה מוגדר היטב.

נשים לב שגם מתקיים

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

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

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 $\text{Aut}(K/\mathbb{Q})$ אל תוך החבורה המתוארת בשאלה 1 ונכתוב את התמונה.
 הוכחה: קודם כל $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ ולכן השיכון הוא $\{1, 3, 5, 7\} \rtimes_\theta (\mathbb{Z}/8\mathbb{Z})$.
 ניקח את האוטומורפיזם שמצאנו בסעיף הקודם, ואז

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

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

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

\square

שאלה 4

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

סעיף א'

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

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

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 להם אלו הם מדרגה 1 ולכן אין להם שורשים מרובים, אז הם ספרבילים ולכן זה פרפקט.

אם נכתוב את f, g בתור פולינומים פורמליים נקבל

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

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

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

ולכן

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

ואז $x \in K(s^{\frac{1}{p}}, t^{\frac{1}{p}}) \subseteq K^{\frac{1}{p}}$ משמע $K^{\frac{1}{p}} \subseteq K(s^{\frac{1}{p}}, t^{\frac{1}{p}})$.

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

נעבור לחשב את הדרגה הנדרשת ונשתמש בכפליות הדרגה

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

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 $[K(s^{\frac{1}{p}}) : K] = p$.
באותו אופן גם $t^{\frac{1}{p}} \notin K(s^{\frac{1}{p}})$ היא שורש של הפולינום $x^p - t$ שהוא שוב אי-פריק ולכן שוב הדרגה היא p ומכפליות הדרגה

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

□

סעיף ב'

נוכיח שלכל $\alpha, \beta \in \overline{\mathbb{F}_p}$ שונים ההרחבות $K(s^{\frac{1}{p}} + \alpha t^{\frac{1}{p}})$ ו- $K(s^{\frac{1}{p}} + \beta t^{\frac{1}{p}})$ שונות זו מזו 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 $x^p = s + \alpha^p t \in K$ ולכן $X^p - (s + \alpha^p t) = 0$ הוא פולינום אי-פריק מעל K כי הוא אי-פריד (כי הנגזרת היא 0 במציין p) ו- x הוא שורש ו- $s + \alpha^p t \notin K^p$ כי אם הוא היה, אז היה מתקיים

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

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 $\alpha \neq \beta$ 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 $\alpha \neq \beta$, 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