פתרון מטלה 07 — מבנים אלגבריים (2), 80446

29 במאי 2025

שאלה 1

נסמן $F=\mathbb{Q}(s)$ ויהי K שדה הפיצול של $x^n-s\in F[x]$.
נראה ש־$\operatorname{Aut}(K/F)\simeq(\mathbb{Z}/n\mathbb{Z})^\times\ltimes_\theta(\mathbb{Z}/n\mathbb{Z})$, כאשר,

$$\theta:(\mathbb{Z}/n\mathbb{Z})^\times\to\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}),\qquad\theta(k)(n)=kn$$

הוכחה. בתרגול ראינו כי מכפלה חצי־ישרה זו היא איזומורפית לחבורת הפונקציות,

$$G=\{f:\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\mid\exists c,d,\ \forall x\in\mathbb{Z}/n\mathbb{Z},\ f(x)=cx+d\}$$

אנו נראה אם כך ש־$G\simeq\operatorname{Aut}(K/F)$. בתרגול כבר ראינו כי קיים שיכון כזה, כלומר מצאנו שזהו הומומורפיזם חד־חד ערכי, ולכן עלינו רק להראות שהומומורפיזם זה הוא גם על. תהי $f\in G$, ונניח ש־c,d קבועים כך ש־$f(x)=cx+d$. אנו יודעים כי $\xi_n^c\in K$ ולכן $\xi_n^m x\mapsto\xi_n^{mc+d}x^c$ הוא אוטומורפיזם תקין, כאשר ההוכחה לטענה זו זהה לזו שראינו בתרגול. נסמן ב־ψ אוטומורפיזם זה ונקבל ש־$G\ni f\mapsto\psi\in\operatorname{Aut}(K/F)$ בדיוק, ובכך נקבל שהומומורפיזם זה אכן על, ובהתאם הוא אוטומורפיזם. $\square$

שאלה 2

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

הוכחה. נניח בשלילה שב־L יש אינסוף שורשי יחידה. בפרט יש אינסוף שורשי יחידה פרימיטיביים, שאם לא כן יש כמות סופית של שורשי יחידה. בלי הגבלת הכלליות נוכל לבחור אינסוף שורשי יחידה פרימיטיביים מסדר ראשוני, אחרת מהעובדה שיש אינסוף שורשים פרימיטיביים נוכל לבחור מכפלות ולבודד ראשוניים. נסמן $\{\xi_{p_i}\}_{i=1}^{\infty}$ שורשי יחידה פרימיטיביים מסדר p_i ראשוני כך ש־$p_i \neq p_j$ לכל $i \neq j$.
ידוע כי $L/\mathbb{Q}$ נוצרת סופית ולכן ישנה כמות סופית של פולינומים המגדירים את ההרחבה, אבל ξ_{p_i} מעיד על הפולינום $x^{p_i} - 1$ כפולינום שניתן לפיצול בהרחבה, ולכן קיבלנו שיש $\{x^{p_i} - 1\}_{i=1}^{\infty}$ פולינומים, בפרט כמות אינסופית, בסתירה. $\square$

שאלה 3

יהי K שדה פיצול של $x^8 - 2$ מעל $\mathbb{Q}$.

סעיף א׳

נראה שניתן לזהות את K עם השדה $\mathbb{Q}(i)(\sqrt[8]{2}) \subseteq \mathbb{C}$, כאשר שורש מוגדר לפי הענף הראשי של השורש.

הוכחה. נבחין כי $\xi_8 \sqrt[8]{2} \in K$, אבל $\xi_8 = e^{\frac{2\pi i}{8}} = \frac{1+i}{\sqrt{2}}$.

$$\left(\xi_8 \sqrt[8]{2}\right)^2 = i \cdot \sqrt[4]{2} \qquad \left(\xi_8 \sqrt[8]{2}\right)^6 = -i \cdot \sqrt[4]{2} \cdot \sqrt{2}$$

ולכן בפרט גם,

$$\left(\xi_8 \sqrt[8]{2}\right)^2 - \left(\xi_8 \sqrt[8]{2}\right)^6 = \sqrt[4]{2} i (1 + \sqrt{2}) \in K$$

וכן,

$$\frac{\sqrt[4]{2} i (1 + \sqrt{2})}{\left(\xi_8 \sqrt[8]{2}\right)^2} 1 + \sqrt{2} \in K$$

ונסיק ש־$\sqrt{2} \in K$. אז גם $(1+i)\sqrt[8]{2} \in K$, אבל באותו אופן תוך שימוש בחזקה שביעית נקבל שגם $(1-i)\sqrt[8]{2} \in K$ ולכן $i, \sqrt[8]{2} \in K$. לכן $K \supseteq \mathbb{Q}(i, \sqrt[8]{2})$, אבל אנו כבר יודעים כי $K \subseteq \mathbb{Q}(i, \sqrt[8]{2})$ ממהלך ההוכחה, ולכן השדות שווים.

נבחין כי טענה זו עד כדי אוטומורפיזם המצמיד לשורשים הפרימיטיביים שבחרנו. □

סעיף ב׳

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

הוכחה. נבחין כי $\mathbb{Q}(i)(\sqrt[8]{2}) = \mathbb{Q}(i)[x]/(x^8 - 2)$ הוא שדה ולכן בפרט $x^8 - 2$ אי־פריק ב־$\mathbb{Q}(i)$. זאת ישירות מהטענה כי $\sqrt[8]{2}$ הוא האיבר שהפולינום המינימלי שלו הוא $x^8 - 2$. □

סעיף ג׳

נוכיח שעבור $\varepsilon \in \{-1, 1\}$ ולכל שורש z של $x^8 - 2$ קיים אוטומורפיזם של K כך ש־$i \mapsto \varepsilon i$ ו־$\sqrt[8]{2} \mapsto z$

הוכחה. נניח ש־$z = \sqrt[8]{2}\xi_8^m$ עבור $0 \le m < n$. ראינו כי $G \simeq \mathrm{Aut}(\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q})$ עבור G משאלה 1.
נגדיר את הפונקציה $f : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ על־ידי,

$$f(x) = (2 + \varepsilon)x + m$$

ולכן משאלה 1 קיים אוטומורפיזם $\iota \in \mathrm{Aut}(\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q})$ כך שמתקיים,

$$\iota(\sqrt[8]{2}) = \xi_8^{(2+\varepsilon)\cdot 0 + m} \sqrt[8]{2} = z$$

בנוסף גם,

$$\iota(i) = \iota(\xi_8^2) = \xi_8^{(2-\varepsilon)\cdot 2} = -1 \cdot \xi_8^{-2\varepsilon} = \varepsilon i$$

ומצאנו אוטומורפיזם המקיים את הרצוי. □

סעיף ד׳

נמצא שיכון של $\mathrm{Aut}(K/\mathbb{Q})$ אל תוך החבורה המתוארת בסעיף א׳ ונמצא את תמונתה.

פתרון נבחין כי $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$ ולכן השיכון הוא לתוך $(\mathbb{Z}/8\mathbb{Z}) \rtimes_\theta \{1, 3, 5, 7\}$ על־ידי אותו שיכון המתואר בסעיף הקודם.

שאלה 4

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

סעיף א׳

נראה ש־$[K^{1/p} : K] = p^2$.

הוכחה. נבחין כי לכל $x \in \overline{\mathbb{F}_p}$ יש שורש p שכן $\overline{\mathbb{F}_p}$ שדה מושלם. בנוסף אנו יודעים כי $s, t \in K$ וכי קיימים $\alpha, \beta \in K^{1/p}$ כך ש־$s = \alpha^p, t = \beta^p$. לכן $[K^{1/p} : K] \geq p^2$. מהצד השני, ידוע כי $(x+y)^p = x^p + y^p$ לכל $x, y \in K$ ולכן נוכל להסיק שלכל $x \in K$ קיים ערך התלוי ב־$\overline{\mathbb{F}_p}, \alpha, \beta$ כך שהוא מעיד על שורש p. נסיק ש־$[K^{1/p} : K] = p^2$ בדיוק. $\square$

סעיף ב׳

נראה שלכל $\alpha, \beta \in \overline{\mathbb{F}_p}$ שונים, ההרחבות $K(s^{1/p} + \alpha t^{1/p})$ ו־$K(s^{1/p} + \beta t^{1/p})$ שונות זו מזו ובעלות דרגה p.
נסיק שיש אינסוף שדות ביניים בין K ל־$K^{1/p}$.

הוכחה. נראה ש־$[K(s^{1/p} + \alpha t^{1/p}) : K] = p$. ברור כי $[K(s^{1/p} + \alpha t^{1/p}) : K] \geq p$ (מכפלת שורשי p) ולכן מספיק לחסום את הביטוי. נבחין כי $(s^{1/p} + \alpha t^{1/p})^p = s + \alpha^p t \in K$ ולכן בהכרח $[K(s^{1/p} + \alpha t^{1/p}) : K] \leq p$ ונסיק שהדרגה היא בדיוק p.

נטען תחילה כי $\alpha^p \neq \beta^p$, זאת שכן $(\alpha+\beta)^p = \alpha^p + \beta^p$. לכן גם $s^{1/p} + \alpha t^{1/p} \neq s^{1/p} + \beta t^{1/p}$. אי־שוויון זה כמובן איננו מספיק כדי להראות שההרחבות שונות זו מזו, נראה שאי־אפשר לבטא ערך אחד על־ידי השני. נניח בשלילה שאפשר, כלומר $s^{1/p} + \beta t^{1/p} \in K(s^{1/p} + \alpha t^{1/p})$, לכן גם $t^{1/p} \in K(s^{1/p} + \alpha t^{1/p})$ על־ידי חיבור וחילוק איברים בשדה. לכן גם $s^{1/p}$ בשדה. אבל נובע שדרגת ההרחבה : $[K(s^{1/p} + \alpha t^{1/p})$ $K] = p \geq p^2$, וזו סתירה, לכן שני השדות אכן שונים.

לבסוף נסיק שיש אינסוף הרחבות ביניים שונות, זאת ישירות מבחירת $\alpha \in \overline{\mathbb{F}_p}$, יש אינסוף כאלה. $\square$