פתרון מטלה 09 — מבנים אלגבריים (2), 80446

9 ביוני 2025

שאלה 1

תהי L/K הרחבה סופית. לכל $\alpha \in L$ נגדיר את הפונקציה $M_\alpha : L \to L$ על־ידי,

$$M_\alpha(x) = \alpha \cdot x$$

בתרגול הגדרנו את הפונקציה $\mathrm{tr}_{L/K} : L \to K$ על־ידי,

$$\mathrm{tr}_{L/K}(\alpha) = \mathrm{tr}(M_\alpha)$$

ובאופן דומה את $N_{L/K} : L \to K$ על־ידי $N_{L/K}(\alpha) = \det(M_\alpha)$.

יהי $\alpha \in L$ עם הפולינום המינימלי $f(x) = x^d + c_1 x^{d-1} + \cdots + c_d$.

נראה בסעיפים הבאים כי,

$$\mathrm{tr}_{L/K}(\alpha) = \frac{[L:K]}{d}, \qquad N_{L/K}(\alpha) = c_d^{[L:K]/d}$$

סעיף א׳

נגדיר את הבסיס,

$$C = (1, x, \ldots, x^{d-1})$$

בסיס ל־$K(\alpha)/K$.

אם $B = (b_1, \ldots, b_t)$ בסיס ל־$L/K(\alpha)$ אז גם,

$$D = (x^i \cdot b_j)_{0 \le i < d, 1 \le j \le t}$$

בסיס ל־L/K.

סעיף ב׳

תהי $T : K(\alpha) \to K(\alpha)$ העתקה לינארית של כפל ב־α.

נראה שמתקיים,

$$[T]_C = \begin{pmatrix} 0 & \cdots & 0 & -c_d \\ 1 & 0 & \cdots & -c_{d-1} \\ & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & -c_1 \end{pmatrix}$$

הוכחה. נבחין כי $x = \alpha$ כווקטור מעל המרחב $K(\alpha)$. עבור $n < d$ מתקיים,

$$T(c_n) = Tx^n = \alpha x^n = x \cdot x^n = x^{n+1}$$

ונבחין במקרה המיוחד $n = d - 1$,

$$x^d = -(c_1 x^{d-1} + \cdots + c_d)$$

ישירות מהגדרת השדה, נכתוב את המטריצה על־פי ערכי הווקטורים שמצאנו ונקבל,

$$[T]_C = \begin{pmatrix} 0 & \cdots & 0 & -c_d \\ 1 & 0 & \cdots & -c_{d-1} \\ & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & -c_1 \end{pmatrix}$$

בדיוק כפי שרצינו. $\square$

סעיף ג׳

נראה שעבור הבסיס D מתקיים,

$$[M_\alpha]_D = \operatorname{diag}([T]_C, \dots, [T]_C)$$

ונסיק את הטענה.

הוכחה. יהי $0 \le i < d$ ו־$1 \le j \le t$, אז,

$$M_\alpha x^i b_j = \alpha \cdot x^i \cdot b_j = x^{i+1} b_j$$

ויחד עם הסעיף הקודם נקבל ישירות את המסקנה המבוקשת.

עתה נוכל לחשב ישירות ונקבל,

$$\operatorname{tr}_{L/K}(\alpha) = [L : K(\alpha)] \cdot (-c_1) = -\frac{[L:K]}{d} c_1$$

ובאופן דומה מחוקי דטרמיננטות,

$$N_{L/K}(\alpha) = (\det [T]_C)^{[L:K]/d} = -c_d^{[L:K]/d}$$

□

סעיף ד׳

נסיק שאם $\alpha_1, \dots, \alpha_d$ הם הצמודים של α ב־$\overline{K}$ אז,

$$\operatorname{tr}_{L/K}(\alpha) = \frac{[L:K]}{d} \sum_{i=1}^{d} \alpha_i$$

וכן,

$$N_{N/K}(\alpha) = \left(\prod_{i=1}^{d} \alpha_i \right)^{[L:K]/d}$$

הוכחה. מתקיים,

$$f(x) = \prod_{i=1}^{d} (x - \alpha_i)$$

ולכן,

$$c_1 = \sum_{i=1}^{d} \alpha_i$$

מחישוב שנעשה במטלות קודמות, נסיק את החלק של הטענה ישירות ממסקנת הסעיף הקודם.

מאותה שאלה ממטלות קודמות גם,

$$c_d = \prod_{i=1}^{d} \alpha_i$$

והחלק השני של הטענה נובע. □

שאלה 2

יהי F שדה ונניח ש־$L = F(t_1, \dots, t_n)$ עם הפעולה של S_n המוגדרת על־ידי,

$$\sigma \cdot P = P(t_{\sigma(1)}, \dots, t_{\sigma(n)})$$

נסמן ב־$s_1, \dots, s_n$ את הפולינומים הסימטריים האלמנטריים ב־$t_1, \dots, t_n$, כלומר הפולינומים המקיימים,

$$\prod_{i=1}^{n}(x - t_i) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n$$

בכל סעיף נגדיר איבר $P \in L^{S_n}$ ונבטא אותו באמצעות הפולינומים הסימטריים האלמנטריים.

סעיף א׳

נגדיר $P = t_1^3 + \cdots + t_n^3$.

פתרון נסמן,

$$Q = \sum_{\substack{1 \le i,j \le n \\ i \ne j}} t_i^2 t_j$$

מחישוב ישיר מתקיים,

$$s_1^3 = P + s_3 + Q \iff P = s_1^3 - s_3 - Q$$

ונבחין כי גם מתקיים,

$$s_1 s_2 = s_3 + Q$$

ולכן,

$$Q = s_1 s_2 - s_3$$

ובהתאם גם,

$$P = s_1^3 - s_1 s_2$$

סעיף ב׳

נגדיר את הפולינום,

$$P = \sum_{\substack{1 \le i,j \le n \\ i \ne j}} t_i^2 t_j$$

פתרון בהתאם לסעיף הקודם,

$$P = s_1 s_2 - s_3$$

סעיף ג׳

עבור $n = 3$ נגדיר,

$$P = ((t_1 - t_2)(t_1 - t_3)(t_2 - t_3))^2$$

פתרון

$$(t_1 - t_2)(t_1 - t_3)(t_2 - t_3) = 4s_3 + (t_1^2 t_2 - t_1^2 t_3 - t_2^2 t_1 + t_2^2 t_3 + t_3^2 t_1 - t_3^2 t_2) = s_2^2 - 2s_3 s_1$$

מבדיקה ישירה, ולכן גם,

$$P = (s_2^2 - ss_3 s_1)^2$$

שאלה 3

סעיף א׳

תהי L/K הרחבת גלואה כך ש־$G=\mathrm{Gal}(L/K)$. נראה שלכל $H\le G$ מתקיים $[L^H:K]=[G:H]$.

הוכחה. אנו כבר יודעים כי $[L:K]=|G|$ וכן שמתקיים,

$$[G:H]=\frac{|G|}{|H|}=\frac{[L:K]}{|H|}=\frac{[L:L^H]\cdot[L^H:K]}{|H|}$$

ולכן ננסה לחשב את $[L:L^H]$.

בהרצאה ראינו את הטענה כי $H=\mathrm{Gal}(L/L^H)$ ולכן ממשפט אפיון גודל חבורת האוטומורפיזמים, $[L:L^H]=|H|$ נקבל אם כך,

$$[G:H]=\frac{[L:L^H]\cdot[L^H:K]}{|H|}=\frac{[L:L^H]\cdot|H|}{|H|}=[L^H:K]$$

בדיוק כפי שרצינו. $\square$

סעיף ב׳

נוכיח של־A_4 אין תת־חבורה מאינדקס 2, ונסיק שאם $\mathrm{Gal}(L/K)\simeq A_4$ אז אין הרחבת ביניים $L/F/K$ כך ש־$[F:K]=2$.

הוכחה. אנו יודעים ש־$|S_4|=4!=24$ וכן ש־$|A_4|=4!/2=12$. אילו הייתה $H\le A_4$ תת־חבורה מאינדקס 2, אז $|H|=6$ בדיוק. בהתאם אנו גם יודעים כי $H\simeq\mathbb{Z}/6\mathbb{Z}$ או $H\simeq S_3$ בלבד. אם $H\simeq\mathbb{Z}/6\mathbb{Z}$ אז יש תמורה $\sigma\in A_4$ מסדר 6, אבל כל תמורה כזו היא מסדר 3 כמחזור מגודל 3, או שני מחזורים מסדר 2, ובהתאם סדר σ הוא 2 או 3 בלבד, ולכן $H\simeq S_3$. בהתאם חייב להיות $\sigma\in S_3$ מסדר 3 ו־$\tau\in S_3$ מסדר 2. בהתאם $\{\sigma,\sigma^2\}\subseteq S_3$ וכן $\{\sigma,\sigma^2,e\}\not\ni\tau^{-1}\sigma\tau\in S_3$ ונקבל ישירות ש־$|H|>6$ בסתירה. לכן לא קיים H כזה.

נניח ש־L/K הרחבת גלואה כך ש־$\mathrm{Gal}(L/K)\simeq A_4$. נניח בשלילה ש־$L/F/K$ כך ש־$[F:K]=2=|H|$ עבור $H\le A_4$ בהתאם לסעיף הקודם. אבל ראינו עתה כי לא קיים H כזה, ולכן בהכרח גם לא קיים F כזה. $\square$