פתרון מטלה 09 — מבנים אלגבריים 2, 80446

15 ביוני 2025

שאלה 1

תהיי L/K. עבור $\alpha \in L$ נסמן $M_\alpha : L \to L$ את הפונקציה $M_\alpha(x)$, אופרטור לינארי על L כמרחב וקטורי מעל K.
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 הפונקציה $N_{L/K} : L \to K$ על־ידי $N_{L/K}(\alpha) = \det(M_\alpha)$.
יהי $\alpha \in L$ עם פולינום מינימלי $f_{\alpha/K}(x) = x^d + c_1 x^{d-1} + + \cdots + c_d$.

סעיף א'

יהי $\mathcal{B} = (b_1, \cdots, b_t)$ בסיס ל־$L/K(\alpha)$. ניזכר מדוע $\mathcal{C} = (1, x, \cdots x^{d-1}$ בסיס ל־$K(\alpha)$ מעל K ומדוע

$$\mathcal{D} = \left(1 \cdot b_1, x \cdot b_1, \cdots x^{d-1} b_1, 1 \cdot b_2, x \cdot b_2, \cdots x^{d-1} b_2, \cdots, 1 \cdot b_t, \cdots x^{d-1} b_t\right)$$

בסיס ל־L/K.

הוכחה: עבור הבסיס $\mathcal{D}$ זה נובע ממגדל הרחבות ומכפלה ישרה של בסיסים ועבור $\mathcal{C}$ הוא בסיס של $K(\alpha)$ מעל K כי $K(\alpha)$ הוא שקול ל־$K[x]/\left(f_{\alpha/K}\right)$ ואנחנו יודעים שהפולינום הזה מדרגה d ולכן גם הבסיס יהיה מסדר d וברגע שנעשה מודלו d על $f_{\alpha/K}$ נקבל

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

כלומר שאם ניקח את הבסיס $\mathcal{C}$ נוכל להציג כל $g \in K(\alpha)$ על־ידו. $\square$

סעיף ב'

תהיי $T : K(\alpha) \to K(\alpha)$ ההעתקה שכופלת כל איבר ב־α.
נראה שעבור בסיס $\mathcal{C}$ מסעיף א' מתקיים

$$[T]_{\mathcal{C}} = \begin{bmatrix} 0 & & & -c_d \\ 1 & \ddots & & \ddots \\ & \ddots & 0 & -c_2 \\ & & 1 & -c_1 \end{bmatrix}$$

הוכחה: היות ו־T העתקה לינארית מתקיים

$$T(\alpha^i) = \alpha \cdot \alpha^i = \alpha^{i+1}$$

וגם

$$T\left(\alpha^{d-1}\right) = \alpha \cdot \alpha^{d-1} = \alpha^d = f_{\alpha/k(\alpha)} - \sum_{i=0}^{d-1} c_i \alpha_i = 0 - \sum_{i=0}^{d-1} c_{d-i} \alpha^i$$

והמטריצה שמייצגת את ההעתקה הלינארית T לפי הבסיס $\mathcal{C}$ היא

$$[T]_{\mathcal{C}} = \begin{bmatrix} 0 & 0 & \cdots & -c_d \\ 1 & 0 & \cdots & -c_{d-1} \\ 0 & 1 & \cdots & -c_{d-2} \\ 0 & 0 & \cdots - c_1 & \end{bmatrix}$$

$\square$

סעיף ג'

נוכיח שעבור הבסיס $\mathcal{D}$ מסעיף א' מתקיים $[M_\alpha]_{\mathcal{D}} = \begin{bmatrix} [T]_{\mathcal{C}} & & 0 \\ & \ddots & \\ 0 & & [T]_{\mathcal{C}} \end{bmatrix}$ ונסיק שמתקיים

$$\mathrm{Tr}_{L/K}(\alpha) = \frac{[L:K]}{d} \cdot (-c_1),\ \ N_{L/K}(\alpha) = \left((-1)^d c_d\right)^{\frac{[L:K]}{d}}$$

כאשר $\frac{[L:K]}{d} = [L:K(\alpha)]$.

הוכחה: ראשית, $\alpha \equiv x$. שנית, יהי $0 \leq i < d$ ו־$1 \leq j \leq t$ אז מתקיים

$$M_\alpha\left(x^i b_j\right) = \alpha \cdot x^i \cdot b_j = x^{i+1} b_j$$

מהסעיף הקודם מתקיים

$$x^{i+1} b_j = \left(-\sum_{i=0}^{d-1} c_{d-i} x^i\right) b_j = \sum_{i=0}^{d-1} (-c_{d-i} x^i) b_j = \sum_{i=0}^{d-1} \left(-c_{d-i} d_i^j\right)$$

כאשר $d_i^j \in \mathcal{D}$, אז נקבל (סליחה שדילגתי על שלב בכתיבה, הסתבכתי עם ה־typst, אבל זה ישיר)

$$\begin{bmatrix} | & | & | & | \\ \left[M_\alpha\left(x^0 b_j\right)\right]_{\mathcal{D}} & \left[M_\alpha\left(x^1 b_j\right)\right]_{\mathcal{D}} & \cdots & \left[M_\alpha\left(x^{d-1} b_j\right)\right]_{\mathcal{D}} \\ | & | & | & | \end{bmatrix} = \begin{bmatrix} [T]_{\mathcal{C}} & & 0 \\ & \ddots & \\ 0 & & [T]_{\mathcal{C}} \end{bmatrix}$$

נעבור לחלק של ההסקה, מתקיים ממה שראינו

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}[M_\alpha]_{\mathcal{D}} = \sum_{i=1}^{t} \mathrm{tr}[T]_{\mathcal{C}} = \sum_{i=1}^{t} (-c_1) = -t c_1 = -[L:K(\alpha)] \cdot c_1 = -\frac{[L:K]}{[K(\alpha):K]} c_1 = -\frac{[L:K]}{d} c_1$$

$$N_{L/K}(\alpha) = \det[M_\alpha]_{\mathcal{D}} = \prod_{i=1}^{t} \det[T]_{\mathcal{C}} = (\det[T]_{\mathcal{C}})^t \underset{\text{פיתוח לפי שורה ראשונה}}{=} (-c_d)^t \underset{t=\left[K:K(\alpha)=\frac{[L:K]}{d}\right]}{=} (-c_d)^{\frac{[L:K]}{d}}$$

□

סעיף ד'

נסיק בנוסף שאם $\alpha_1, \cdots, \alpha_d$ הם צמודים של α בסגור אלגברי של K אז

$$\mathrm{Tr}_{L/K}(\alpha) = \frac{[L:K]}{d} \sum_i \alpha_i,\ \ N_{L/K}(\alpha) = \left(\prod_i \alpha_i\right)^{\frac{[L:K]}{d}}$$

הוכחה: מההנחה מתקיים

$$\prod_{i=1}^{d} (x - \alpha_i) = f_{\alpha/K}(x) = x^d + c_1 x^{d-1} + \cdots + c_d$$

ואז $c_1 = \sum_{i=1}^{d} \alpha_i, c_d = (-1)^d \prod_{i=1}^{d} \alpha_i$ וממה שמצאנו בסעיף א'

$$\mathrm{Tr}_{L/K}(\alpha) = -\frac{[L:K]}{d} c_1 = -\frac{[L:K]}{d} \sum_{i=1}^{d} \alpha_i$$

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

□

שאלה 2

יהי F שדה ויהי $L = F(t_1, \cdots, t_n)$ עם הפעולה S_n המוגדרת על־ידי $\sigma.P(t_1, \cdots, t_n) = P\left(t_{\sigma(1)}, \cdots t_{\sigma(n)}\right)$.
נסמן ב־$s_1, \cdots, s_n$ את הפולינומים הסימטריים האלמנטריים ב־$t_1, \cdots, t_n$ אלו הפולינומים המקיימים

$$\prod_{i=1}^{n}(x - t_i) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n$$

בכל אחד מהסעיפים נתון איבר P ב־L^{S_n} ונבטא אותו באמצעות הפולינומים הסימטריים האלמנטריים.
תזכורת: הנוסחה שראינו בתרגול למציאת הפולינום הסימטרי s_n עבור k נעלמים היא

$$s_n = \sum_{1 \le i_1 < i_2 < \cdots < i_n \le k} \left(x_{i_1} \cdots x_{i_k}\right)$$

סעיף א'

$P = t_1^3 + t_2^3 + \cdots + t_n^3$.
פתרון: ראשית, P פולינום סימטרי (שכן כל החזקות אותו הדבר ולכן שינוי מיקום הסכימה לא משנה את סדר הסכימה).
נעבוד כמו בתרגול: בצעד הראשון, ניקח את $f - s_1^2$ כאשר $s_1 = t_1 + t_2 + t_3$.
נחשב את s_1^3

$$s_1^3 = (t_1 + \cdots + t_n)^3 \underset{\text{נוסחת הבינום}}{=} \sum_{i=1}^{n} t_i^3 + 3 \sum_{1 \le i < j \le n} t_i^2 t_j + 3 \sum_{1 \le i < j \le n} t_i t_j^2 + 6 \sum_{1 \le i < j < k \le n} t_i t_j t_k$$

אז בסך־הכל כרגע יש לנו

$$\begin{aligned} f - s_1^3 &= t_1^3 + \cdots + t_n^3 - \left(\sum_{i=1}^{n} t_i^3 + 3 \sum_{1 \le i < j \le n} t_i^2 t_j + 3 \sum_{1 \le i < j \le n} t_i t_j^2 + 6 \sum_{1 \le i < j < k \le n} t_i t_j t_k \right) \\ &= -\left(3 \sum_{1 \le i < j \le n} t_i^2 t_j + 3 \sum_{1 \le i < j \le n} t_i t_j^2 + 6 \sum_{1 \le i < j < k \le n} t_i t_j t_k \right) \end{aligned}$$

כעת נשים לב שמתקיים (זה בגלל חישוב של פתיחת סוגריים ומהגדרה)

$$3 \sum_{1 \le i < j \le n} t_i^2 t_j + 3 \sum_{1 \le i < j \le n} t_i t_j^2 = 3 \sum_{1 \le i < j \le n} t_i t_j (t_1 + \cdots + t_n) = 3 s_2 s_1$$

הגורם האחרון שנשאר לנו לבטא באמצעות הפולינומים הסימטריים הוא כמובן

$$6 \sum_{1 \le i < j < k \le n} t_i t_j t_k = 6 s_3$$

מצאנו שבסך־הכל מתקיים

$$P = t_1^3 + \cdots t_n^3 = s_1^3 - 3 s_1 s_2 + 6 s_3$$

□

סעיף ב'

$.P=\sum_{1\leq i\neq j\leq n}t_it_j^2$

פתרון: קודם כל, P אכן פולינום סימטרי (אפשר לראות כבר עבור $n=2$), ולכן נשתמש במשפט היסודי.

נפרק את P לביטוי שיהיה לנו נוח יותר לעבודה:

$$P=\sum_{1\leq i\neq j\leq n}t_it_j^2=\sum_{i=1}^n t_i\sum_{i\neq j}t_j^2=\sum_{i=1}^n t_i\left(\sum_{j=1}^n t_j^2-t_i^2\right)=\sum_{i=1}^n t_i\sum_{j=1}^n t_j^2-\sum_{i=1}^n t_i^3$$

זה ביטוי שיותר נוח לנו :דרך מפורשת יותר להגיד שלכל $i\in[n]$ אנחנו סוכמים את כל המכפלות של t_i עם כל t_j עבור $j\neq i$, זאת־אומרת שאנחנו **לא** רוצים את חזקות 3 של t_i בסכום שלנו, ובצורה הזאת הפולינומים הסימטריים הנדרשים נובעים כמעט ישירות:

מהסעיף הקודם

$$\sum_{i=1}^n t_i^3=s_1^3-3s_1s_2++6s_3$$

ניקח $i\in[n]$ ונשים לב שמתקיים

$$\sum_{\substack{1\leq j\leq n\\ i\neq j}}t_j^2=s_1^2-2s_2=(t_1+\cdots t_n)^2-2\sum_{1\leq k<l\leq n}t_kt_l$$

וכמובן

$$\sum_{i=1}^n t_i=s_1$$

נרכיב ביחד ונקבל

$$P=\sum_{1\leq i\neq j\leq n}t_it_j^2=\sum_{i=1}^n t_i\sum_{j=1}^n t_j^2-\sum_{i=1}^n t_i^3=s_1(s_1^2-2s_2)-(s_1^3-3s_1s_2+6s_3)\underset{s_1s_2=s_2s_1}{=}\cancel{s_1^3}-2s_1s_2-\cancel{s_1^3}+3s_1s_2-6s_3$$
$$=s_1s_2-6s_3$$

$\square$

סעיף ג'

$.P=[(t_1-t_2)(t_1-t_3)(t_2-t_3)]^2$

פתרון: נתחיל מלחשב את הביטוי הפנימי

$$(t_1-t_2)(t_1-t_3)(t_2-t_3)=(t_1^2-t_1t_3-t_2t_1+t_2t_3)(t_2-t_3)=t_1^2t_2-t_1^2t_3+t_1(t_3^2-t_2^2)+t_2^2t_3-t_2t_3^2$$

נעלה בריבוע

$$(t_1^2t_2-t_1^2t_3+t_1(t_3^2-t_2^2)+t_2^2t_3-t_2t_3^2)(t_1^2t_2-t_1^2t_3+t_1(t_3^2-t_2^2)+t_2^2t_3-t_2t_3^2)$$
$$=t_1^4t_2^2-2t_1^4t_2t_3+t_1^4t_3^2-2t_1^3t_2^3+2t_1^3t_2^2t_3+2t_1^3t_2t_3^2-2t_1^3t_3^3$$
$$+t_1^2t_2^4+2t_1^2t_2^3t_3-6t_1^2t_2^2t_3^2+2t_1^2t_2t_3^3+t_1^2t_3^4-2t_1t_2^4t_3+2t_1t_2^3t_3^2+2t_1t_2^2t_3^3-2t_1t_2t_3^4+t_2^4t_3^2-2t_2^3t_3^3+t_2^2t_3^4$$

קצת מגעיל אבל ניגש לעבודה; נראה לי הכי כדאי להתחיל עם החזקות הרביעיות, ולכן נפתח את הביטוי $.s_1^2s_2^2$

$$s_1^2=(t_1+t_2+t_3)^2=t_1^2+t_2^2+t_3^2+2(t_1t_2+t_2t_3+t_1t_3)=t_1^2+t_2^2+t_3^2+2s_2$$
$$s_2^2=(t_1t_2+t_1t_3+t_2t_3)^2=t_1^2t_2^2+t_1^2t_3^2+t_2^2t_3^2+2(x_1x_2x_1x_3+x_1x_2x_2x_3+x_1x_3x_2x_3)=t_1^2t_2^2+t_1^2t_3^2+t_2^2t_3^2+2s_1t_1t_2t_3$$
$$s_1^2s_2^2=(t_1^2+t_2^2+t_3^2+2s_2)(t_1^2t_2^2+t_1^2t_3^2+t_2^2t_3^2+2s_1t_1t_2t_3)$$
$$=t_1^4t_2^2+2t_1^4t_2t_3+t_1^4t_3^2+2t_1^3t_2^3+8t_1^3t_2^2t_3+8t_1^3t_2t_3^2+2t_1^3t_3^3+t_1^2t_2^4$$
$$+8t_1^2t_2^3t_3+15t_1^2t_2^2t_3^2+8t_1^2t_2t_3^3+t_1^2t_3^4+2t_1t_2^4t_3+8t_1t_2^3t_3^2+8t_1t_2^2t_3^3+2t_1t_2t_3^4+t_2^4t_3^2+2t_2^3t_3^3+t_2^2t_3^4$$
$$P-s_1^2s_2^2=-4t_1^4t_2t_3-4t_1^3t_2^3-6t_1^3t_2^2t_3-6t_1^3t_2t_3^2-4t_1^3t_3^3-6t_1^2t_2^3t_3-21t_1^2t_2^2t_3^2-6t_1^2t_2t_3^3-4t_1t_2^4t_3-6t_1t_2^3t_3^2-6t_1t_2^2t_3^3-4t_1t_2t_3^4-4t_2^3t_3^3$$

מאותן סיבות כמקודם, נוריד $-4s^3s_3$ ונקבל

$$P - s_1^2s_2 - (-4s^3s_3) = 4t_1^4t_2^4t_3 + 12t_1^4t_2^3t_3^2 + 12t_1^4t_2^2t_3^3 + 4t_1^4t_2t_3^4 - 4t_1^4t_2t_3 + 12t_1^3t_2^4t_3^2 + 24t_1^3t_2^3t_3^3 - 4t_1^3t_2^3 + 12t_1^3t_2^2t_3^4 - 6t_1^3t_2^2t_3$$
$$-6t_1^3t_2t_3^2 - 4t_1^3t_3^3 + 12t_1^2t_2^4t_3^3 + 12t_1^2t_2^3t_3^4 - 6t_1^2t_2^3t_3 - 21t_1^2t_2^2t_3^2 - 6t_1^2t_2t_3^3 + 4t_1t_2^4t_3^4 - 4t_1t_2^4t_3 - 6t_1t_2^3t_3^2 - 6t_1t_2^2t_3^3 - 4t_1t_2t_3^4 - 4t_2^3t_3^3$$

עכשיו נוריד $-4s_2^3$ ומההפרש נקבל

$$4t_1^4t_2^4t_3 + 12t_1^4t_2^3t_3^2 + 12t_1^4t_2^2t_3^3 + 4t_1^4t_2t_3^4 - 4t_1^4t_2t_3 + 12t_1^3t_2^4t_3^2 + 24t_1^3t_2^3t_3^3 + 12t_1^3t_2^2t_3^4 + 6t_1^3t_2^2t_3 + 6t_1^3t_2t_3^2 + 12t_1^2t_2^4t_3^3$$
$$+12t_1^2t_2^3t_3^4 + 6t_1^2t_2^3t_3 + 3t_1^2t_2^2t_3^2 + 6t_1^2t_2t_3^3 + 4t_1t_2^4t_3^4 - 4t_1t_2^4t_3 + 6t_1t_2^3t_3^2 + 6t_1t_2^2t_3^3 - 4t_1t_2t_3^4$$

נשאר להוריד $12s_1s_2s_3$ וגם $-27s_3^2$, בסך הכל קיבלנו:

$$P = s_1^2s_2^2 - 4s_1^3s_3 - 4s_2^3 + 12s_1s_2s_3 - 27s_3^2$$

□

שאלה 3

סעיף א'

תהיי L/K הרחבת גלואה כך ש־$\mathrm{Gal}(L/K)=G$. נשתמש בהתאמת גלואה כדי להוכיח שלכל $H\leq G$ מתקיים $[L^H:K]=[G:H]$.

הוכחה: ראשית, אנחנו עובדים עם הרחבות סופיות בלבד לפי הערה שמיכאל אמר. אז בלי הגבלת הכלליות, ההרחבת גלואה L/K היא הרחבה סופית.

מהתאמת גלואה אנחנו יודעים שיש התאמה חד־חד ערכית ועל בין תתי חבורות של G לבין שדות ביניים של ההרחבה L/K ובפרט שאם $H\leq G$ אז L^H הוא שדה ביניים בין K לבין L (כי $K\subseteq L^H\subseteq L$ כי $K\subseteq L^H$ כי K מכיל את כל האיברים שנשמרים תחת כל האוטומורפיזמים ב־G, בפרט אלו ב־H) ולכן לפי טענה שראינו בהרצאה מתקיים גם $H=\mathrm{Gal}(L/L^H)$ ונובע על־כן $|H|=[L:L^H]$.

נשתמש בטענות על מגדל הרחבות וכפליות הדרגה

$$[L:K]=[L:L^H]\cdot[L^K:K]$$

מהתאמת גלואה נובע גם $[L:K]=|G|$ אז בסך־הכל

$$[L:K]=|G|=|H|\cdot[L^k:K]=[L:L^H]\cdot[L^K:K]$$

ולכן

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

□

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: ראשית, תת־חבורה מאינדקס 2 בA_4 היא מסדר 6 ($|A_4|=\frac{4!}{2}=12, \frac{|A_4|}{2}=6$).

נניח כי יש תת־חבורה כזאת, ואנחנו כבר יודעים שיש רק 2 חבורות מסדר 6 בידיוק (לפי משפטי סילו) וזה או $\mathbb{Z}_6$ או S_3.

נניח כי יש תת־חבורה כזאת H ולכן מלגראנז' נקבל ש־$H\lhd A_4$.

אז $g^2\in H$ לכל $g\in A_4$ ולכן כל 3־מחזור $(a,b,c)\in A_4$ מתקיים $(a,b,c)^2\in H$ ולכן כל ה־3 מחזורים של A_4 הם גם ב־H.

אבל מספר ה־3־מחזורים ב־A_4 נתונים על־ידי

$$\binom{4}{3}\cdot 2!=8$$

ולכן ב־H יש שמונה איברים, אבל זאת סתירה.

עבור החלק השני, נניח ש־L/K הרחבת גלואה ו־$\mathrm{Gal}(L/K)\simeq A_4$, ולכן מהתאמת גלואה אנחנו יודעים שלכל $H\leq A_4$ יש התאמה חד־חד ערכית ועל אל $K\subseteq L^H$ וראינו בסעיף הקודם שמתקיים $[L^H:K]=[A_4:H]$.

אם הייתה הרחבת ביניים $L/F/K$ כך ש־$[F:K]=2$, היה נובע כי ה־H המתאימה לה מהתאמת גלואה היא חבורה נורמלית ב־A_4 וראינו שזה לא אפשרי.

□