פתרון מטלה 10 — מבנים אלגבריים 2, 80446

21 ביוני 2025

שאלה 1

יהי $f \in \mathbb{Q}[x]$ פולינום אי־פריק מדרגה 3 ויהי L שדה הפיצול.

נוכיח ש־$[L:\mathbb{Q}] = 3$ אם ורק אם D_f ריבוע ב־$\mathbb{Q}$ ואחרת $[L:\mathbb{Q}] = 6$.

הוכחה: נתחיל מלהראות אם האם ורק אם ואחרי זה נראה את האחרת.

$\Longleftarrow$ נניח כי $[L:\mathbb{Q}] = 3$ ונרצה להראות ש־$D_f \in \mathbb{Q}$.

מהתאמת גלואה אנחנו יודעים ש־$\mathrm{Gal}(L/\mathbb{Q}) \leq S_3$, נסביר למה: $\mathrm{Gal}(L/\mathbb{Q})$ מכילה את כל האוטומורפיזמים של L שמשמרים את $\mathbb{Q}$, והם בעצם מבצעים תמורות על השורשים של f שמדרגה 3 ולכן יש לו שלושה שורשים $\alpha_1, \alpha_2, \alpha_3$ שמהטרנזטיביות יכולים לעבור לשורש אחר והאוטומורפיזמים מכבדים כמובן את מבנה החבורה ולכן $\mathrm{Gal}(L/\mathbb{Q}) \leq S_3$.

ל־S_3 יש שישה איברים ולכן ממשפט לגראנז' $|\mathrm{Gal}(L/\mathbb{Q})| \mid 6 = |S_3|$ וגם $\mathrm{Gal}(L/\mathbb{Q})$ צריכה להיות טרנזטיבית ולכן $\mathrm{Gal}(L/\mathbb{Q})$ היא או S_3 עצמה או A_3, הראשונה כמובן לא אפשרית כי $[L:\mathbb{Q}] = 3$ ולכן $\mathrm{Gal}(L/\mathbb{Q}) = A_3$.

מהגדרת הדיסקרמיננטה נקבל

$$D_f = \prod_{i<j} \left(\alpha_i - \alpha_j\right)^2 \in \mathbb{Q}$$

ונשים לב ש־$\sqrt{D_f} = \prod_{i<j} (\alpha_i - \alpha_j)$ הוא פולינום סימטרי ואינווריאנטי תחת תמורות זוגיות ולכן $\sqrt{D_f} \in L$ ובכלל שהחבורת גלואה כי A_3 כל האוטומורפיזמים של החבורת גלואה משמרים את $\sqrt{D_f}$ ולכן $\sqrt{D_f} \in \mathbb{Q} \Rightarrow D_f = \left(\sqrt{D_f}\right)^2 \in \mathbb{Q}^2$, כנדרש.

$\Longrightarrow$ בכיוון השני, נניח כי $D_f \in \mathbb{Q}^2$ ונרצה להראות ש־$[L:\mathbb{Q}] = 3$.

מההנחה, $\sqrt{D_f} \in \mathbb{Q}$ ומהגדרה $\sqrt{D_f} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ כאשר כמקודם $\alpha_1, \alpha_2, \alpha_3$ שורשים של f.

אבל מכך ש־$\sqrt{D_f} \in \mathbb{Q}$ זה אומר שהוא נשמר תחת כל האוטומורפיזמים, ו־$\sqrt{D_f}$ הוא אנטי־סימטרי (כי החלפה בסדר של ביטוי פנימי במכפלה משנה סימן), ולכן $\sqrt{D_f}$ נשמר רק תחת תמורות זוגיות ולכן $\mathrm{Gal}(L/\mathbb{Q}) \subseteq A_3$, אבל זה בהכרח גורר כי $\mathrm{Gal}(L/\mathbb{Q}) \simeq A_3$ כי חבורת גלואה היא טרנזטיבית וכמובן כתת־חבורה היא צריכה לחלק את הסדר, אבל ל־A_3 אין תתי־חבורות טרנזטיביות מלבד עצמה.

אז

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq A_3 \Rightarrow |\mathrm{Gal}(L/\mathbb{Q})| = 3 \Rightarrow [L:\mathbb{Q} = 3$$

וזה סוגר את החלק הראשון, עבור החלק השני גם נראה את שני הכיוונים:

$\Longleftarrow$ נניח כי $[L:\mathbb{Q}] = 6$ ונראה כי $D_f \notin \mathbb{Q}^2$.

מאותם נימוקים לעיל נובע כי $\mathrm{Gal}(L/\mathbb{Q}) = S_3$ (עם ההנחה נפסלת האפשרות של A_3), ולכן תמורות אי־זוגיות משנות את הסימן

$$\sigma\left(\sqrt{D_f}\right) = -\sqrt{D_f}$$

וזה בהכרח אומר כי $\sqrt{D_f} \notin \mathbb{Q}$ כי הוא לא נשמר תחת כל האוטומורפיזמים מחבורת גלואה ולכן $D_f \notin \mathbb{Q}^2$.

$\Longrightarrow$ בכיוון השני, נניח כי $D_f \notin \mathbb{Q}^2$ ונראה כי $[L:\mathbb{Q}] = 6$.

אז $\sqrt{D_f}$ משנה סימן תחת האוטומורפיזמים של חבורת גלואה, אבל הטרנזטיביות כמובן צריכה להישמר ומכיוון שחלק מהאוטומורפיזמים משנים סימן נובע שהחבורת גלואה מכילה תמורות אי־זוגיות ולכן היא לא A_3 ונשאר רק $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$ ולכן $[L:\mathbb{Q}] = 6$. $\square$

שאלה 2

יהיו F שדה ממציין שונה מ־2, $f \in F[x]$ פולינום ספרבילי אי־פריק ומתוקן ו־L שדה הפיצול של f מעל F.
נסמן ב־$\alpha_1, \cdots \alpha_n$ את שורשי f ב־L ונגדיר $K = F\left(\sqrt{D_f}\right)$ כאשר $D_f = \prod_{1 \le i < j \le n} \left(\alpha_i - \alpha_j\right)^2$ היא הדיסקרמיננטה של f.
נוכיח שמתקיים

$$\mathrm{Gal}(L/K) = \left\{\sigma \in \mathrm{Gal}(L/F) \mid \sigma \underset{\{\alpha_1, \cdots \alpha_n\}}{\restriction} \text{תמורה זוגית}\right\}$$

כלומר, אם מזהים את $\mathrm{Gal}(L/F)$ עם תמונתה בחבורת התמורות ($S_n \simeq \mathrm{Sym}(\{\alpha_1, \cdots, \alpha_n\})$) אז $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/F) \cap A_n$.
הוכחה: מהיות L שדה הפיצול של f ומכך ש־f פולינום ספרבילי, אי־פריק ומתוקן כל אוטומורפיזם ב־$\mathrm{Gal}(L/F)$ הוא תמורה על שורשי f, ולכן

$$\sigma \cdot \alpha_i := \sigma(\alpha_i)$$

וזה מביא לנו הומומורפיזם כפי שראינו לחבורת התמורות, ונטען שהפעולה לעיל היא פעולה נאמנה: בעצם, $\sigma = \mathrm{Id}$ וזה כי: L נוצר על־ידי השורשים $\alpha_1, \cdots, \alpha_n$, ולכן אם σ נקבע על־ידי $\alpha_1 \cdots \alpha_n$ הוא מקבע את כל איברי L, לכן $\mathrm{Gal}(L/F) \hookrightarrow S_n$ (הגרעין של ההומומורפיזם הוא טריוויאלי ולכן חד־חד ערכי והפעולה נאמנה. היא כמובן גם טרנזטיבית כי הפולינום f הוא אי־פריק וספרבילי ולפי טענה שראינו זה אומר שחבורת גלואה פועלת בצורה טרנזטיבית במקרה זה על השורשים של הפולינום).
אז $\mathrm{Gal}(L/F)$ הוא תת־חבורה של חבורת התמורות וכל $\sigma \in \mathrm{Gal}(L/F)$ מקיימת $\sigma : \alpha_i \mapsto \alpha_{\sigma(i)}$.
אם נסתכל על הדיסקרמיננטה נקבל

$$\sqrt{D_f} = \prod_{i<j} (\alpha_i - \alpha_j) \underset{\sigma \in \mathrm{Gal}(L/F)}{\Rightarrow} \sqrt{D_f} \overset{\sigma}{\mapsto} \prod_{i<j} \left(\sigma(\alpha_i) - \sigma\left(\alpha_j\right)\right) = \prod_{i<j} \left(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}\right) = \mathrm{sgn}(\sigma) \cdot \sqrt{D_f}$$

זאת־אומרת $\sigma\left(\sqrt{D_f}\right) = \sqrt{D_f}$ אם σ תמורה זוגית ו־$\sigma\left(\sqrt{D_f}\right) = -\sqrt{D_f}$ אם σ תמורה אי־זוגית.
אז נגדיר

$$H := \left\{\sigma \in \mathrm{Gal}(L/F) \mid \sigma\left(\sqrt{D_f}\right) = \sqrt{D_f}\right\} \underset{\text{מהנימוק למעלה על זוגיות}}{=} \{\sigma \in \mathrm{Gal}(L/F) \mid \mathrm{sgn}(\sigma) = +1\}$$

אבל נשים לב ש־$H = \mathrm{Gal}(L/K)$! למה? כי $K = F\left(\sqrt{D_f}\right)$ משמע כל σ מקבעת את $\sqrt{D_f}$ (מהמשפט היסודי של תורת גלואה).
נשים לב שבידיוק מתקיים אם כך $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/F) \cap A_n$. $\square$

שאלה 3

יהיו F שדה, $f \in F[x]$ פולינום ספרבילי, אי־פריק ומתוקן ו־L שדה הפיצול של f מעל F.
אם $0 \neq p = \mathrm{char}(F)$, נניח ש־$n = |\mathrm{Gal}(L/F)| \nmid p$ ותהיי $H \leq \mathrm{Gal}(L/F)$.

סעיף א'

נגדיר העתקה לינארית $A_H : L \to L$ על־ידי $A_H(x) = \frac{1}{|H|}\sum_{\sigma \in H} \sigma(x)$.
נוכיח ש־A_H היא הטלה על L^H, כלומר $\mathrm{Im}(A_H) = L^H$ ו־$A_H \underset{L^H}{\restriction} = \mathrm{Id}_{L^H}$
הוכחה: נתחיל מלהראות ש־$\mathrm{Im}(A_H) = L^H$ באמצעות הכלה דו־כיוונית:
$\mathrm{Im}(A_H) \subseteq L^H$: נרצה להראות שלכל $x \in L$ מתקיים $A_H(x) \in L^H$, בשביל זה ניקח $\tau \in H$ ונחשב עבור $x \in L$ שרירותי

$$\tau(A_H(x)) = \tau\left(\frac{1}{|H|}\sum_{\sigma \in H}\sigma(x)\right) \underset{|H|=m}{=} \frac{1}{m}\sum_{\sigma \in H}(\tau\sigma)(x) \underset{\{\tau\sigma \ | \ \sigma \in H\} = H \text{ חבורה ולכן } H}{=} \frac{1}{m}\sum_{\sigma \in H}\sigma(x)$$

זה אומר ש־$A_H(x) \in L^H$ לכל $x \in L$ ומביא לנו את ההכלה בכיוון הזה.
$L^H \subseteq \mathrm{Im}(A_H)$: מספיק שנראה ש־$A_H \underset{L^H}{\restriction} = \mathrm{Id}_{L^H}$.
ניקח $x \in L^H$ ולכן לכל $\sigma \in H$ מתקיים $\sigma(x) = x$, אז

$$A_H(x) = \frac{1}{|H|}\sum_{\sigma \in H}\sigma(x) \underset{|H|=m}{=} \frac{1}{m} \cdot m \cdot x = x$$

ולכן $A_H \underset{L^H}{\restriction} \mathrm{Id}_{L^H}$, וזה גם אומר שלכל $y \in L$ מתקיים $A_H(y) = y$ וזה מביא לנו את ההכלה בכיוון השני.
מצאנו הכלה דו־כיוונית ולכן $\mathrm{Im}(A_H) = L^H$ ולכן A_H היא הטלה על L^H. $\square$

סעיף ב'

נסיק שאם $\mathcal{B} = (b_1, \cdots b_n)$ בסיס ל־L מעל F אזי $\mathrm{Spna}(A_H(b_1), \cdots A_H(b_n)) = L^H$.
הוכחה: נראה באמצעות הכלה דו־כיוונית:
$\mathrm{Span}(A_H(b_1), \cdots, A_H(b_n)) \subseteq L^H$: ניקח $b_i \in \mathcal{B}$, אז מתקיים

$$A_H(b_i) = \frac{1}{|H|}\sum_{\sigma \in H}\sigma(b_i) \in L^H$$

וזה סוגר את ההכלה בכיוון הזה, זה כבר נובע מתהליכים שעשינו בסעיף א' אבל ארשום שוב: כי אם ניקח $\tau \in H$ נקבל

$$\tau(A_H(b_i)) = \sigma\left(\frac{1}{|H|}\sum_{\sigma \in H}\sigma(b_i)\right) = \frac{1}{m}\sum_{\sigma \in H}(\tau\sigma)(b_i) \underset{H \text{ חבורה}}{=} \frac{1}{m}\sum_{\rho \in H}\rho(b_i) = A_H(b_i)$$

$\tau \in H$ שרירותי וקיבלנו ש־$\tau(A_H(b_i)) = A_H(b_i)$ ולכן זה נכון לכל $\tau \in H$ ולכן $A_H(b_i) \in L^H = \{x \in L \mid \sigma(x) = x \forall \sigma \in H\}$.
$\mathrm{Span}(A_H(b_1), \cdots, A_H(b_n)) \supseteq L^H$: ניקח $b_i \in \mathcal{B}$: ניקח $y \in L^H$, בגלל ש־$\mathcal{B}$ בסיס ל־L מעל F, מתקיים

$$y = \sum_{i=1}^{n} c_i b_i \ \ (c_i \in F)$$

בפרט מתקיים

$$A_H(y) = A_H\left(\sum_{i=1}^{n} c_i b_i\right) = \sum_{i=1}^{n} c_i A_H(b_i)$$

אבל מסעיף א' אנחנו יודעים שמתקיים $A_H(y) = y$ ולכן

$$y = \sum_{i=1}^{n} c_i A_H(b_i)$$

וזה מביא לנו את ההכלה בכיוון השני.
הראינו הכלה דו־כיוונית ולכן $\mathrm{Spna}(A_H(b_1), \cdots A_H(b_n)) = L^H$. $\square$

סעיף ג'

נמצא דוגמה ל־F, f, L, H כבשאלה ו־$\alpha \in L$ כך ש־$L = F(\alpha)$ אבל $F(A_H(\alpha)) \not\subseteq L^H$.

הוכחה: נגדיר

$$F = \mathbb{Q}, f(x) = x^3 - 2, \alpha = \xi_3 \sqrt[3]{2}, L^H = F(\xi_3)$$

וכן

$$H = A_3 = \{\xi_3 \mapsto \xi_3^i \mid 0 \leq i \leq 2\}$$

ונקבל

$$A_H(\alpha) = \frac{1}{3} \sum_{\sigma \in H} \sigma(\alpha) = \frac{1}{3} \sum_{i=0}^{2} \xi_3^i \sqrt[3]{2} = 0$$

ואז

$$F(A_H(\alpha)) = F(0) = F \not\subseteq L$$

$\square$

שאלה 4

נביט בפולינום $f(x)=x^4-7x^2+7\in\mathbb{Q}[x]$.

בתרגיל 8 ראינו שחבורת גלואה של שדה הפיצול L של f איזומורפית ל־D_4.

אם β_1,β_2 הם השורשים של $y^2-7y+7=0$ אז $\pm\sqrt{\beta_1},\pm\sqrt{\beta_2}$ הם ארבעת שורשי f (שמוגדרים היטב כי β_1,β_2 ממשיים חיוביים).

נמצא את שמונה התמורות של השורשים שמושרות מאיברי $\mathrm{Gal}(L/\mathbb{Q})$.

הוכחה: נעזר ברמז: לא ייתכן ש־$\sigma\in\mathrm{Gal}(L/\mathbb{Q})$ תקיים $\sigma\left(\sqrt{\beta_1}\right)\in\left\{\sqrt{\beta_2},-\sqrt{\beta_2}\right\}$ ו־$\sigma\left(-\sqrt{\beta_1}\right)\in\left\{\sqrt{\beta_1},-\sqrt{\beta_1}\right\}$ כי חייב להתקיים $\sigma\left(\sqrt{\beta_1}\right)+\sigma\left(-\sqrt{\beta_1}\right)=\sigma\left(\sqrt{\beta_1}-\sqrt{\beta_1}\right)=0$, ונפעיל שיקולים דומים כדי לפסול את כל התמורות פרט ל־8.

מהרמז אנחנו מקבלים $\sigma\left(-\sqrt{\beta_1}\right)=-\sigma\left(\sqrt{\beta_1}\right)$, ולכן אם $\sigma\left(\sqrt{\beta_1}\right)=\sqrt{\beta_2}$ אז $\sigma\left(-\sqrt{\beta_1}\right)=-\sqrt{\beta_2}$, ואז נקבל שגם מתקיים $\sigma\left(\sqrt{\beta_1}\right),\sigma\left(-\sqrt{\beta_1}\right)\in\left\{\pm\sqrt{\beta_2}\right\}$.

נשים לב שלא ייתכן $\sqrt{\beta_1}\mapsto\sqrt{\beta_2}$ וגם $-\sqrt{\beta_1}\mapsto-\sqrt{\beta_1}$ כי אז $\sigma\left(\sqrt{\beta_1}\right)+\sigma\left(-\sqrt{\beta_1}\right)=\sqrt{\beta_2}-\sqrt{\beta_1}\neq 0$ אז כבר מצאנו תמורה לא תקינה.

גם אם נמשיך ונכתוב את הקומבינציות האלו ידנית נגיע לתמורות לא כשרות; זאת מכיוון שחבורת גלואה צריכה למפות כל זוג $\left\{\sqrt{\beta_i},-\sqrt{\beta_i}\right\}$ לזוג מתאים בצורה 'קונסיסטנטית' זאת אומרת שאם $\sqrt{\beta_1}\mapsto\sqrt{\beta_2}$ אז חייב שיתקיים גם $-\sqrt{\beta_1}\mapsto-\sqrt{\beta_2}$ (כמובן אפשר גם להחליף בין הצמדים האלו, זאת־אומרת $\sqrt{\beta_1}\mapsto-\sqrt{\beta_2},-\sqrt{\beta_1}\mapsto\sqrt{\beta_2}$), או לחילופין תמורת הזהות $\sqrt{\beta_1}\mapsto\sqrt{\beta_1}$ או התמורה מחליפת סימן $\sqrt{\beta_1}\mapsto-\sqrt{\beta_1}$.

אז כל תמורה חייבת לשמר את הזוג או להחליף אותו בשלמותו עם זוג אחר – אין אמצע.

קומבינטורית, יש לנו 2 זוגות של שורשים $\left\{\pm\sqrt{\beta_1}\right\},\left\{\pm\sqrt{\beta_2}\right\}$, ויש לנו את אחת מהאופציות הבאות:

1. או שאנחנו מחליפים בין הזוגות ויש לכך 2 אופציות
2. בצורה בלתי תלויה, להחליף בין הסימנים בתוך כל זוג ולכן יש לנו 2 אפשרויות בכל זוג

זה באמת נותן לנו $2\cdot2\cdot2=8$ אפשרויות כמו שנדרשנו למצוא, נרשום בצורה ישירה (לכתוב טבלאות זה קשה):

מספר תמורה	החלפת זוגות	שינוי סימן $\left\{\pm\sqrt{\beta_1}\right\}$	שינוי סימן $\left\{\pm\sqrt{\beta_2}\right\}$	מיפוי
σ_1	X	X	X	$\sqrt{\beta_1}\mapsto\sqrt{\beta_1},-\sqrt{\beta_1}\mapsto-\sqrt{\beta_1}$ $\sqrt{\beta_2}\mapsto\sqrt{\beta_2},-\sqrt{\beta_2}\mapsto-\sqrt{\beta_2}$
σ_2	X	✓	X	$\sqrt{\beta_1}\mapsto-\sqrt{\beta_1},-\sqrt{\beta_1}\mapsto\sqrt{\beta_1}$ $\sqrt{\beta_2}\mapsto\sqrt{\beta_2},-\sqrt{\beta_2}\mapsto-\sqrt{\beta_2}$
σ_3	X	X	✓	$\sqrt{\beta_1}\mapsto\sqrt{\beta_1},-\sqrt{\beta_1}\mapsto-\sqrt{\beta_1}$ $\sqrt{\beta_2}\mapsto-\sqrt{\beta_2},-\sqrt{\beta_2}\mapsto\sqrt{\beta_2}$
σ_4	X	✓	✓	$\sqrt{\beta_1}\mapsto-\sqrt{\beta_1},-\sqrt{\beta_1}\mapsto\sqrt{\beta_1}$ $\sqrt{\beta_2}\mapsto-\sqrt{\beta_2},-\sqrt{\beta_2}\mapsto\sqrt{\beta_2}$
σ_5	✓	X	X	$\sqrt{\beta_1}\mapsto\sqrt{\beta_2},-\sqrt{\beta_1}\mapsto-\sqrt{\beta_2}$ $\sqrt{\beta_2}\mapsto\sqrt{\beta_1},-\sqrt{\beta_2}\mapsto-\sqrt{\beta_1}$
σ_6	✓	✓	X	$\sqrt{\beta_1}\mapsto-\sqrt{\beta_2},-\sqrt{\beta_1}\mapsto\sqrt{\beta_2}$ $\sqrt{\beta_2}\mapsto\sqrt{\beta_1},-\sqrt{\beta_2}\mapsto-\sqrt{\beta_1}$
σ_7	✓	X	✓	$\sqrt{\beta_1}\mapsto\sqrt{\beta_2},-\sqrt{\beta_1}\mapsto-\sqrt{\beta_2}$ $\sqrt{\beta_2}\mapsto-\sqrt{\beta_1},-\sqrt{\beta_2}\mapsto\sqrt{\beta_1}$
σ_8	✓	✓	✓	$\sqrt{\beta_1}\mapsto-\sqrt{\beta_2},-\sqrt{\beta_1}\mapsto\sqrt{\beta_2}$ $\sqrt{\beta_2}\mapsto-\sqrt{\beta_1},-\sqrt{\beta_2}\mapsto\sqrt{\beta_1}$

$\square$