

## פתרון תרגיל בית 8 בשדות ותורת גלואה 88-311 סמסטר א' תש"ף

**שאלה 1.** כהכנה לאחרי חנוכה, שחקו ב"אוקלידס: המשחק" (או בקישור הזה) והגיעו לפחות לשלב 6. הרבה יותר נוח להשתמש במחשב נייד או נייד מאשר בטלפון.

**שאלה 2.** למי שרוצה להתנסות בעוד משחק של בניות בסרגל ומחוגה מוזמן לנסות את המשחק Euclidean. זה מספיק ממכר שכדאי לוודא שנשאר זמן לשאר תרגיל הבית.

**שאלה 3.** תהי  $E = \mathbb{Q}[\alpha]/\mathbb{Q}$  הרחבת גלואה. נניח שיש  $\sigma \in \text{Gal}(E/\mathbb{Q})$  כך ש- $\sigma(\alpha) = \alpha^2$ .

א. האם ייתכן כי  $[E : \mathbb{Q}] = 2$ ? אם כן, מצאו  $\alpha$  מתאים.

ב. האם ייתכן כי  $[E : \mathbb{Q}] = 3$ ? אם כן, מצאו  $\alpha$  מתאים.

פתרון.

א. נניח שיש שדה  $E$  כזה. זו הרחבת גלואה ולכן  $|\text{Gal}(E/\mathbb{Q})| = 2$ . אז  $\alpha \notin \mathbb{Q}$  ולכן  $\alpha^2 \neq \alpha$ , כלומר  $\sigma \neq \text{id}$ . בהכרח  $\sigma$  מסדר 2, ולכן

$$\alpha = \sigma^2(\alpha) = \sigma(\alpha^2) = \alpha^4$$

כלומר  $\alpha = \alpha^4$ . לכן  $\alpha^3 = 1$  וקיבלנו ש- $\alpha$  הוא שורש יחידה פרימיטיבי מסדר 3. זה יתכן, כמו שראינו בכיתה שאם  $E = \mathbb{Q}[\rho_3]$ , אז  $[E : \mathbb{Q}] = 2$ .

ב. נניח שיש שדה  $E$  כזה. לכן  $|\text{Gal}(E/\mathbb{Q})| = 3$ . לכן  $\sigma$  היא מסדר 3. לכן

$$\alpha = \sigma^3(\alpha) = \alpha^8$$

כלומר  $\alpha^7 = 1$ . אבל אז  $E = \mathbb{Q}[\rho_7]$  וראינו כי  $[\mathbb{Q}[\rho_7] : \mathbb{Q}] = 6$ , וזו סתירה.

**שאלה 4.** יהי  $f(x) \in \mathbb{Q}[x]$  פולינום אי פריק עם שדה פיצול  $E$ . נניח שחבורת גלואה  $\text{Gal}(E/\mathbb{Q})$  היא אבלית. יהי  $a$  שורש של  $f(x)$ .

א. הוכיחו כי  $\mathbb{Q}(a)/\mathbb{Q}$  הרחבת גלואה.

ב. הוכיחו כי  $E = \mathbb{Q}(a)$ .

פתרון. ניתן להחליף את  $\mathbb{Q}$  בשדה אחר  $F$ , עם הדרישה שהרחבה  $E/F$  היא גלואה.

א. ההרחבה  $\mathbb{Q}(a)/\mathbb{Q}$  היא גלואה אם ורק אם  $\text{Gal}(E/\mathbb{Q}(a)) \leq \text{Gal}(E/\mathbb{Q})$  היא תת-חבורה נורמלית. היא אכן נורמלית כי  $\text{Gal}(E/\mathbb{Q})$  אבלית, ולכן כל תת-חבורה שלה נורמלית.

ב. נסמן את שורשי הפולינום  $f(x)$  ב- $a_1, \dots, a_k$ . חבורת גלואה פועלת טרנזיטיבית על קבוצת השורשים. כלומר לכל  $i$  יש  $\varphi \in \text{Gal}(E/\mathbb{Q})$  כך ש- $\varphi(a) = a_i$ . אבל מפני ש- $\mathbb{Q}(a)/\mathbb{Q}$  נורמלית אפשר לצמצם את  $\varphi$  ל- $\mathbb{Q}(a)$ , ולכן  $\varphi|_{\mathbb{Q}(a)}(a) = a_i \in \mathbb{Q}(a)$ . לכל  $i$ . כלומר  $\mathbb{Q}(a)$  שווה לשדה הפיצול  $E$ .

**שאלה 5.** יהי  $F$  שדה ממאפיין שונה מ-2, ויהי  $K$  שדה הפיצול של פולינום מתוקן ספרבילי  $f(x) \in F[x]$ . נסמן את שורשי  $f(x)$  ב- $\alpha_1, \dots, \alpha_n$ . נגדיר את הדיסקרימיננטה של  $f(x)$  להיות

$$\Delta(f) := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

א. בדקו שהדיסקרימיננטה של  $x^2 + bx + c$  זה מה שאתם חושבים שזה. להראות שהדיסקרימיננטה של  $x^3 + ux + v \in \mathbb{Q}[x]$  היא  $4u^3 + 27v^2$  זו רשות שהיא קצת יותר קשה. הדיסקרימיננטה כשמה כן היא: לפולינומים ב- $\mathbb{R}$  היא "מאבחנת" את מספר השורשים הממשיים.

ב. הוכיחו כי  $\Delta(f) \in F$ . רמז: חילופים ב- $S_n$ .

ג. נתבונן ב- $G := \text{Gal}(K/F)$  כתת-חבורה של  $S_n$ , ונסמן  $G_0 = G \cap A_n$ . הוכיחו כי  $F[\sqrt{\Delta(f)}] = K^{G_0}$ . רמז: מה היא ההגדרה של תמורה זוגית?

ד. הסיקו כי  $G$  משוכנת ב- $A_n$  אם ורק אם  $\sqrt{\Delta(f)} \in F$ .

פתרון.

א. השורשים  $x^2 + bx + c$  הם  $(-b \pm \sqrt{b^2 - 4ac})/2$  ולכן

$$\Delta(x^2 + bx + c) = \left( \frac{-b + \sqrt{b^2 - 4ac}}{2} - \frac{-b - \sqrt{b^2 - 4ac}}{2} \right)^2 = \left( \frac{2\sqrt{b^2 - 4ac}}{2} \right)^2 = b^2 - 4ac$$

ב. נראה כי  $\text{Gal}(K/F) \hookrightarrow S_n$  שומר על הדיסקרימיננטה. נזכר כי  $S_n$  נוצרת על ידי חילופים מהצורה  $(i, i+1)$  ולכן מספיק להראות שהם שומרים על הדיסקרימיננטה. אכן, החילוף  $(i, i+1)$  שומר על כל הגורמים שאין בהם את  $\alpha_i$  או  $\alpha_{i+1}$ . את  $(\alpha_i - \alpha_{i+1})^2$  הוא שולח ל- $(\alpha_i - \alpha_{i+1})^2 = (\alpha_{i+1} - \alpha_i)^2$ , ובנוסף הוא מחליף בין הגורמים  $(\alpha_i - \alpha_j)^2 \leftrightarrow (\alpha_{i+1} - \alpha_j)^2$  ובין הגורמים  $(\alpha_j - \alpha_i)^2 \leftrightarrow (\alpha_j - \alpha_{i+1})^2$ . בסך הכל  $S_n$  שומרת על המכפלה  $\Delta(f)$ , ולכן על חבורת גלואה, ומכאן  $\Delta(f) \in F$ . כדורש,  $K^G = F$ .

ג. לפי החישובים מהסעיף הקודם, החילוף  $(i, i+1)$  שולח את  $\sqrt{\Delta(f)}$  ל- $-\sqrt{\Delta(f)}$ . כידוע, ניתן לכתוב כל תמורה כמכפלה של חילופים ולכן נקבל  $\sigma(\sqrt{\Delta(f)}) = \text{sign}(\sigma)\sqrt{\Delta(f)}$ . אם כן,  $\sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)}$  אם ורק אם  $\text{sign}(\sigma) = 1$  אם ורק אם  $\sigma \in A_n$ .

מכאן נסיק כי  $F[\sqrt{\Delta(f)}] \subseteq K^{G_0}$ , ומצד שני  $G_0 \subseteq \text{Gal}(K/F[\sqrt{\Delta(f)}])$ . לפי התאמת גלואה זה מוכיח את הדרוש. היה אפשר להוכיח במקום, באופן דומה לסעיף הקודם, כי  $\sqrt{\Delta(f)}$  שומר על תמורות זוגיות על ידי זה שנראה כי הוא שומר על מחזורים מהצורה  $(i, i+1, i+2)$  שיוצרים את  $A_n$ .

ד. לפי הסעיף הקודם והתאמת גלואה: מתקיים  $G_0 = G$  אם ורק אם  $K^{G_0} = K^G = F$ . אם ורק אם  $F[\sqrt{\Delta(f)}] = F$  אם ורק אם  $\sqrt{\Delta(f)} \in F$ .

**שאלה 6** (רשות לא קשה). יהיו שני פולינומים

$$f(x) = x^4 - 10x^2 + 1, \quad g(x) = (x^2 - 2)(x^2 - 3)$$

ראינו שיש להם את אותו שדה פיצול  $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ . כמוכן שחבורת גלואה  $G = \text{Gal}(E/\mathbb{Q})$  פועלת על השורשים של  $f(x), g(x)$ . הזכרו כי השורשים של  $f(x)$  הם  $\pm\sqrt{2} \mp \sqrt{3}, \pm\sqrt{2} \pm \sqrt{3}$  וש של  $g$  הם  $\pm\sqrt{2}, \pm\sqrt{3}$ . הוכיחו כי הפעולות לא איזומורפיות. רמז: בשפה פשוטה מבקשים להראות שלא משנה איך נמספר את השורשים, הפעולות שונות. אפשר קודם לשים לב שתת-החבורות המתאימות ב- $S_4$  אינן צמודות למשל.

פתרון. כבר ראינו שחבורת גלואה של הפולינומים מכילה 4 תמורות והן נקבעות לפי הפעולה על  $\sqrt{2}, \sqrt{3}$ . נזכר שחבורת גלואה של ההרחבה היא  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . נסמן את האיברים שלה כאשר  $\{\text{id}, \theta, \tau, \theta\tau\}$

$$\begin{aligned} \theta(\sqrt{2}) &= -\sqrt{2}, & \theta(\sqrt{3}) &= \sqrt{3} \\ \tau(\sqrt{2}) &= \sqrt{2}, & \tau(\sqrt{3}) &= -\sqrt{3} \end{aligned}$$

אם מסתכלים על זה כתמורות על השורשים  $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$  של  $g(x)$ . אז מתקבלות התמורות

$$\text{id}, (12), (34), (12)(34)$$

ואם מסתכלים על זה כתמורות על השורשים  $\sqrt{2} + \sqrt{3}, -\sqrt{2} + \sqrt{3}, \sqrt{2} - \sqrt{3}, -\sqrt{2} - \sqrt{3}$  אז מתקבלות התמורות

$$\text{id}, (12)(34), (13)(24), (14)(23)$$

בשני המקרים החבורה איזומורפית ל- $\mathbb{Z}_2 \times \mathbb{Z}_2$ . אבל בפעולה השניה לכל איבר בחבורה חוץ מ- $\text{id}$  אין נקודות שבת ובפעולה הראשונה זה לא נכון, ולכן הן לא איזומורפיות. אולי יותר קל לשים לב כי הפעולה הראשונה טרנזיטיבית, והשנייה לא. או לפי זה שבמקרה הראשון החבורה מכילה תמורות אי זוגיות, ואילו במקרה השני מדובר בתת-חבורה של  $A_4$ .

בהצלחה!