

# אלגברה מופשטת 3 – תרגיל 9 – פיתרון

## שאלה 1

יהי  $\rho_n = \exp\left(\frac{2\pi i}{n}\right)$  ויהי  $p$  ראשוני.

- הראו כי קבוצת שורשי היחידה ה- $p$ -פרימיטיביים היא בסיס ל- $\mathbb{Q}[\rho_p]$  מעל  $\mathbb{Q}$ .
- חשבו בעזרת סעיף 1 או בכל דרך אחרת:
  - $[\mathbb{Q}[\rho_7 + \rho_7^2 + \rho_7^4] : \mathbb{Q}]$  .a
  - $[\mathbb{Q}[\rho_{11} + \rho_{11}^{-1}] : \mathbb{Q}]$  .b
  - $[\mathbb{Q}[\rho_5] : \mathbb{Q}[\rho_5 + \rho_5^3]]$  .c
- האם קבוצת שורשי היחידה ה- $n$ -פרימיטיביים היא בסיס ל- $\mathbb{Q}[\rho_n]$  מעל  $\mathbb{Q}$  גם כאשר  $n$  פריק? נמקו את קביעתכם.

## פיתרון

**סעיף 1:** הפולינום המינילי של  $\rho_p$  הוא ממעלה  $p - 1$  ולכן  $\varphi(p) = p - 1$  ולכן  $1, \rho_p^1, \rho_p^2, \dots, \rho_p^{p-2}$  בסיס ל- $\mathbb{Q}[\rho_p]$  מעל  $\mathbb{Q}$ . שורשי היחידה ה- $p$ -פרימיטיביים הם  $\rho_p^1, \rho_p^2, \dots, \rho_p^{p-1}$ . זו קבוצה בגודל  $p - 1$  ולכן כדי להראות שהיא בסיס מספיק להראות שהיא פורשת את  $\mathbb{Q}[\rho_p]$ . לשם כך מספיק להראות ש- $1, \rho_p^1, \rho_p^2, \dots, \rho_p^{p-2} \in \text{span}\{\rho_p^1, \rho_p^2, \dots, \rho_p^{p-1}\}$  עבור  $1, \rho_p^1, \rho_p^2, \dots, \rho_p^{p-2}$ . זה ברור. היות ו- $\rho_p$  שורש של  $x^{p-1} + x^{p-2} + \dots + x + 1$  מתקיים  $x^{p-1} + x^{p-2} + \dots + x + 1 = -\rho_p - \rho_p^2 - \dots - \rho_p^{p-1}$  ולכן גמרנו. **משל.**

**סעיף 2:** נשתמש בעובדה ש- $Gal(\mathbb{Q}[\rho_n]/\mathbb{Q}) \cong U_n$  כאשר האיזומורפיזם נתון ע"י  $\sigma_i \mapsto \rho_n^i$  ו- $i \in U_n$ . ציינו מספר פעמים בכיתה שלכל הרחבת גלואה  $E/F$  ולכל  $\alpha \in E$  המימד  $[F[\alpha] : F]$  הוא מספר צמודי גלואה של  $\alpha$  מעל  $F$  וכך נחשב את המימד של ההרחבות בתת-סעיפים a, b, c. בנוסף, נשתמש בסעיף 1 שאומר ש- $\{\rho_p^1, \rho_p^2, \dots, \rho_p^{p-1}\}$  היא בסיס ל- $\mathbb{Q}[\rho_p]$  כדי להסיק שהצמודים אכן שונים (הם יהיו צירופים לינאריים שונים של אברי הבסיס הזה).

**תת-סעיף a:**  $Gal(\mathbb{Q}[\rho_7]/\mathbb{Q}) = \{\sigma_1, \dots, \sigma_6\}$

$$\sigma_1 = id \text{ ולכן } \sigma_1(\rho_7 + \rho_7^2 + \rho_7^4) = \rho_7 + \rho_7^2 + \rho_7^4$$

$$\sigma_2(\rho_7 + \rho_7^2 + \rho_7^4) = \rho_7^2 + \rho_7^4 + \rho_7^8 = \rho_7^2 + \rho_7^4 + \rho_7 = \rho_7 + \rho_7^2 + \rho_7^4$$

$$\sigma_3(\rho_7 + \rho_7^2 + \rho_7^4) = \rho_7^3 + \rho_7^6 + \rho_7^{12} = \rho_7^3 + \rho_7^6 + \rho_7^5 = \rho_7^3 + \rho_7^5 + \rho_7^6$$

$$\sigma_4(\rho_7 + \rho_7^2 + \rho_7^4) = \rho_7^4 + \rho_7^8 + \rho_7^{16} = \rho_7^4 + \rho_7 + \rho_7^2 = \rho_7 + \rho_7^2 + \rho_7^4$$

$$\sigma_5(\rho_7 + \rho_7^2 + \rho_7^4) = \rho_7^5 + \rho_7^{10} + \rho_7^{20} = \rho_7^5 + \rho_7^3 + \rho_7^6 = \rho_7^3 + \rho_7^5 + \rho_7^6$$

$$\sigma_6(\rho_7 + \rho_7^2 + \rho_7^4) = \rho_7^6 + \rho_7^{12} + \rho_7^{24} = \rho_7^6 + \rho_7^5 + \rho_7^3 = \rho_7^3 + \rho_7^5 + \rho_7^6$$

לכן, ל- $\mathbb{Q}[\rho_7 + \rho_7^2 + \rho_7^4] : \mathbb{Q}$  כלומר 2, שני צמודי גלואה שונים מעל  $\mathbb{Q}$ .

**תת סעיף b:** בתרגיל בית 5, שאלה 1, סעיף 2, הוכחנו שדרגת הפולינום המינימלי של  $\rho_p + \rho_p^{-1}$  מעל  $\mathbb{Q}$  היא  $\frac{p-1}{2}$  לכל  $p$  ראשוני. עבור  $p = 11$  נקבל שהדרגה היא 5 ולכן  $[\mathbb{Q}[\rho_{11} + \rho_{11}^{-1}]: \mathbb{Q}] = 5$ .

פיתרון מלא ללא קיצורי דרך:  $Gal(\mathbb{Q}[\rho_{11}]/\mathbb{Q}) = \{\sigma_1, \dots, \sigma_{10}\}$ .

$$\sigma_1(\rho_{11} + \rho_{11}^{-1}) = \rho_{11} + \rho_{11}^{-1} = \rho_{11} + \rho_{11}^{10} \text{ ולכן } \sigma_1 = id$$

$$\sigma_3(\rho_{11} + \rho_{11}^{-1}) = \rho_{11}^3 + \rho_{11}^{-3} = \rho_{11}^3 + \rho_{11}^8, \sigma_2(\rho_{11} + \rho_{11}^{-1}) = \rho_{11}^2 + \rho_{11}^{-2} = \rho_{11}^2 + \rho_{11}^9$$

$$\sigma_5(\rho_{11} + \rho_{11}^{-1}) = \rho_{11}^5 + \rho_{11}^{-5} = \rho_{11}^5 + \rho_{11}^6, \sigma_4(\rho_{11} + \rho_{11}^{-1}) = \rho_{11}^4 + \rho_{11}^{-4} = \rho_{11}^4 + \rho_{11}^7$$

$$\sigma_7(\rho_{11} + \rho_{11}^{-1}) = \rho_{11}^7 + \rho_{11}^{-7} = \rho_{11}^7 + \rho_{11}^4, \sigma_6(\rho_{11} + \rho_{11}^{-1}) = \rho_{11}^6 + \rho_{11}^{-6} = \rho_{11}^6 + \rho_{11}^5$$

$$\sigma_9(\rho_{11} + \rho_{11}^{-1}) = \rho_{11}^9 + \rho_{11}^{-9} = \rho_{11}^9 + \rho_{11}^2, \sigma_8(\rho_{11} + \rho_{11}^{-1}) = \rho_{11}^8 + \rho_{11}^{-8} = \rho_{11}^8 + \rho_{11}^3$$

$$\sigma_{10}(\rho_{11} + \rho_{11}^{-1}) = \rho_{11}^{10} + \rho_{11}^{-10} = \rho_{11} + \rho_{11}^{10}$$

קיבלנו של- $\rho_{11} + \rho_{11}^{-1}$  מעל  $\mathbb{Q}$  ולכן  $[\mathbb{Q}[\rho_{11} + \rho_{11}^{-1}]: \mathbb{Q}] = 5$ .

**תת סעיף c:**  $Gal(\mathbb{Q}[\rho_5]/\mathbb{Q}) = \{\sigma_1, \dots, \sigma_4\}$ .

$$\sigma_1(\rho_5 + \rho_5^3) = \rho_5 + \rho_5^3 \text{ ולכן } \sigma_1 = id$$

$$\sigma_2(\rho_5 + \rho_5^3) = \rho_5^2 + \rho_5^6 = \rho_5 + \rho_5^2$$

$$\sigma_3(\rho_5 + \rho_5^3) = \rho_5^3 + \rho_5^9 = \rho_5^3 + \rho_5^4$$

$$\sigma_4(\rho_5 + \rho_5^3) = \rho_5^4 + \rho_5^{12} = \rho_5^2 + \rho_5^4$$

קיבלנו של- $\rho_5 + \rho_5^3$  יש 4 צמודים שונים מעל  $\mathbb{Q}$  ולכן  $[\mathbb{Q}[\rho_5 + \rho_5^3]: \mathbb{Q}] = 4$ , לכן,

$$[\mathbb{Q}[\rho_5]: \mathbb{Q}[\rho_5 + \rho_5^3]] = \frac{[\mathbb{Q}[\rho_5]: \mathbb{Q}]}{[\mathbb{Q}[\rho_5 + \rho_5^3]: \mathbb{Q}]} = \frac{4}{4} = 1$$

**סעיף 3:** לא תמיד. לדוגמא, כאשר  $n = 4$ , קבוצת שורשי היחידה ה-4 פרימיטיביים היא  $\{\pm i\}$  וזו קבוצה תלויה לינארית מעל  $\mathbb{Q}$  ובפרט לא בסיס.

## שאלה 2

תהי  $K/F$  הרחבת גלואה ו- $\alpha \in K$ . הוכיחו כי  $K = F[\alpha]$  אם ורק אם לכל  $\sigma \in Gal(K/F)$  מתקיים  $\sigma\alpha \neq \alpha$ . [רמז: גם הרחבת גלואה].

## הוכחה

כוון א: נניח ש- $K = F[\alpha]$ . יהי  $\sigma \in Gal(K/F)$  כך ש- $\sigma\alpha = \alpha$ , אזי  $\sigma \in Gal(K/F[\alpha])$ . אבל  $Gal(K/F[\alpha]) = \{id\}$  כי  $K/F[\alpha]$  חרבת גלואה (כי  $K/F$  גלואה) ולכן  $[K:F[\alpha]] = 1$ , כלומר,  $\sigma = id$ . לכן, לכל  $\sigma \neq id$  מתקיים  $\sigma\alpha \neq \alpha$ .

כוון ב: נניח כי לכל  $\sigma \in Gal(K/F)$  מתקיים  $\sigma\alpha \neq \alpha$ . יהי  $\sigma \in Gal(K/F[\alpha])$ . אזי  $\sigma\alpha = \alpha$  ולכן  $\sigma = id$ . זה אומר ש- $Gal(K/F[\alpha]) = \{id\}$ . היות ו- $K/F[\alpha]$  גלואה, נובע ש- $[K:F[\alpha]] = 1$  ולכן  $K = F[\alpha]$ . **משל.**

**הערה:** ההוכחה הבאה עבור כוון ב היא שגויה: נסמן  $n = [K:F] = |Gal(K/F)|$  היות ולכל  $id \neq \sigma \in Gal(K/F)$  מתקיים  $\sigma\alpha \neq \alpha$  אז ל- $\alpha$  יש  $n$  צמודים שונים ולכן  $[F[a]:K] = n$ . לפיכך,  $[K:F[a]] = \frac{[K:F]}{[F[a]:F]} = \frac{n}{n} = 1$  וגמרנו.

המעבר השגוי בהוכחה הוא במסקנה של- $\alpha$  יש  $n$  צמודים שונים אם  $\sigma\alpha \neq \alpha$  לכל  $\sigma \in Gal(K/F)$ . ההוכחה של זה לוקחת משפט אחד אך יש לציין אותה.

### שאלה 3

שכנעו את עצמכם בעובדה הבאה:  $\rho_3 \in \mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}]$ .

אתם רשאים להשתמש בפתרון התרגיל בעובדה הבאה: הפולינום המינימלי של  $\sqrt[3]{9 - \sqrt{-3}}$  מעל  $\mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}]$  הוא  $x^3 - (9 - \sqrt{-3})$ .

יהי  $K$  שדה הפיצול של  $x^6 - 18x^3 + 84$  מעל  $\mathbb{Q}$ .

- מצאו את כל האיברים  $\sigma \in Gal(K/\mathbb{Q})$  המקיימים  $\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \sqrt[3]{9 - \sqrt{-3}}$ . עליכם להציג כל איבר ב-2 דרכים: ע"י תיאור לאן נשלח כל אחד מהיוצרים של ההרחבה  $K/\mathbb{Q}$  וע"י התמורה שהוא משרה על שורשי הפולינום  $x^6 - 18x^3 + 84$ . [המלצה: בדקו מהו  $\sigma(\rho_3)$ ].
- הראו כי האיברים שמצאתם בסעיף 1 יוצרים את  $Gal(K/\mathbb{Q})$ . הראו גם כי  $Gal(K/\mathbb{Q})$  אינה אבלית, אך היא אינה איזומורפית ל- $D_9$  (רמז: מצאו תכונה המתקיימת רק עבור  $D_9$ ).
- האם  $K = \mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}} + \sqrt[3]{9 - \sqrt{-3}}]$ ?
- בנוסף:** הביעו את  $Gal(K/\mathbb{Q})$  ע"י יוצרים ויחסים (לכל היותר שלושה יוצרים). הוכיחו את קביעתכם. (כלומר, הראו שהחבורה המתקבלת מהיוצרים ומהיחסים אכן איזומורפית ל- $Gal(K/\mathbb{Q})$ ).

### פתרון

**הערה:**  $\rho_3 \in \mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}]$  כי  $\rho_3 = \frac{1 + \sqrt{-3}}{2} \in \mathbb{Q}[\sqrt{-3}]$  ו- $\sqrt{-3} = (\sqrt[3]{9 + \sqrt{-3}})^3 - 9 \in \mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}]$ .

**הערה:** קיימים שני שורשים שונים ל- $3 - \sqrt{-3}$  ושלושה שורשים שונים ל- $9 + \sqrt{-3}$ . כאשר נדבר על  $\sqrt{-3}$  ו- $\sqrt[3]{9 + \sqrt{-3}}$  הכוונה תהיה לשורש מסוים מתוך השניים/שלושה שבחרנו מראש. החלפת שורש זה לשורש אחר לא תשפיע על התשובות לתרגיל.

**סעיף 1:** אם  $a$  הוא שורש של הפולינום  $x^6 - 18x^3 + 84$ , אז  $a^3 = \frac{18 \pm \sqrt{324 - 336}}{2} = 9 \pm \sqrt{-3}$ . לכן,

שורשי הפולינום  $x^6 - 18x^3 + 84$  הם

$$\alpha_1 = \sqrt[3]{9 + \sqrt{-3}}, \alpha_2 = \rho_3 \sqrt[3]{9 + \sqrt{-3}}, \alpha_3 = \rho_3^2 \sqrt[3]{9 + \sqrt{-3}},$$

$$\alpha_4 = \sqrt[3]{9 - \sqrt{-3}}, \alpha_5 = \rho_3 \sqrt[3]{9 - \sqrt{-3}}, \alpha_6 = \rho_3^2 \sqrt[3]{9 - \sqrt{-3}}$$

(זה גם יהיה המספור שלהם). לכן,

$$K = \mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}, \sqrt[3]{9 - \sqrt{-3}}, \rho_3] = \mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}, \sqrt[3]{9 - \sqrt{-3}}] \quad (\rho_3 \in \mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}] \text{ כי})$$

יהי  $\sigma \in Gal(K/\mathbb{Q})$  המקיים  $\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \sqrt[3]{9 - \sqrt{-3}}$  אזי

$$\sigma(\sqrt{-3}) = \sigma\left(\left(\sqrt[3]{9 + \sqrt{-3}}\right)^3 - 9\right) = \left(\sqrt[3]{9 - \sqrt{-3}}\right)^3 - 9 = -\sqrt{-3}$$

לכן,  $\sigma(\rho_3) = \sigma\left(\frac{1 + \sqrt{-3}}{2}\right) = \frac{1 - \sqrt{-3}}{2} = \rho_3^2$

נסמן  $b = \sigma(\sqrt[3]{9 - \sqrt{-3}})$ . נתון כי הפולינום המינימלי של  $\sqrt[3]{9 - \sqrt{-3}}$  מעל  $\mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}]$  הוא  $x^3 - (9 - \sqrt{-3})$  ולכן הפולינום המינימלי של  $b$  הוא  $x^3 - (9 + \sqrt{-3})$ . זה אומר ש- $b \in \{\alpha_1, \alpha_2, \alpha_3\}$ . לפי טענה שאמרנו בכיתה (והוכחתם בתרגיל בית 6 שאלה 2 סעיף 3), עבור כל  $b \in \{\alpha_1, \alpha_2, \alpha_3\}$  אכן קיים  $\sigma \in Gal(K/\mathbb{Q})$  כך ש- $b = \sigma(\sqrt[3]{9 - \sqrt{-3}})$  וגם  $\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \sqrt[3]{9 - \sqrt{-3}}$  (הערה: ניתן להוכיח את קיום האפשרויות גם משיקולי ספירה – לא קשה לראות כי חייבות להיות לפחות שלוש  $\sigma$ -ות שונות המקיימות  $\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \sqrt[3]{9 - \sqrt{-3}}$ ), לכן, האיברים  $\sigma \in Gal(K/\mathbb{Q})$  המקיימים  $\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \sqrt[3]{9 - \sqrt{-3}}$  הם:

| סימון      | ייצוג ע"י היוצרים   | ייצוג ע"י תמורה |
|------------|---|-----------------|
| $\sigma_1$ | $\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \sqrt[3]{9 - \sqrt{-3}}$<br>$\sigma(\sqrt[3]{9 - \sqrt{-3}}) = \sqrt[3]{9 + \sqrt{-3}}$          | (1,4)(2,6)(3,5) |
| $\sigma_2$ | $\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \sqrt[3]{9 - \sqrt{-3}}$<br>$\sigma(\sqrt[3]{9 - \sqrt{-3}}) = \rho_3 \sqrt[3]{9 + \sqrt{-3}}$   | (1,4,2,6,3,5)   |
| $\sigma_3$ | $\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \sqrt[3]{9 - \sqrt{-3}}$<br>$\sigma(\sqrt[3]{9 - \sqrt{-3}}) = \rho_3^2 \sqrt[3]{9 + \sqrt{-3}}$ | (1,4,3,5,2,6)   |

הסבר קצר לתמורות: לכל  $\sigma$  המקיימת  $\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \sqrt[3]{9 - \sqrt{-3}}$  מתקיים  $\sigma(\rho_3) = \rho_3^2$  ולכן

$$-\sigma(\alpha_2) = \sigma(\rho_3)\sigma(\sqrt[3]{9 + \sqrt{-3}}) = \rho_3^2 \sqrt[3]{9 - \sqrt{-3}} = \alpha_6$$

$$\sigma(\alpha_3) = \sigma(\rho_3)^2 \sigma(\sqrt[3]{9 + \sqrt{-3}}) = \rho_3^4 \sqrt[3]{9 - \sqrt{-3}} = \alpha_5$$

**סעיף 2:** נחשב את  $|Gal(K/\mathbb{Q})|$ : הפולינום  $x^6 - 18x^3 + 84$  אי פריק מעל  $\mathbb{Q}$  כי הוא אייזנשטיין ביחס ל-3. לכן,  $[\mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}] : \mathbb{Q}] = 6$ . הפולינומים המינימלי של  $\sqrt[3]{9 - \sqrt{-3}}$  מעל  $\mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}]$  הוא ממעלה 3 (זה נתון) ולכן  $[K : \mathbb{Q}[\sqrt[3]{9 + \sqrt{-3}}]] = 3$ . לכן,  $[K : \mathbb{Q}] = 3 \cdot 6 = 18$ . היות ו- $K/\mathbb{Q}$  גלואה (כשדה פיצול),  $|Gal(K/\mathbb{Q})| = [K : \mathbb{Q}] = 18$ .

נגדיר  $\alpha = \sigma_1 \sigma_2$  ו- $\beta = \sigma_2 \sigma_1$ . בדקו שהתמורה המתאימה ל- $\alpha$  היא (4,6,5) והתמורה המתאימה ל- $\beta$  היא (1,2,3). אלו שני מחזורים זרים מסדר 3 ב- $S_6$  ולכן הם יוצרים חבורה בגודל 9 (בפרט, נובע ש- $|\langle \alpha, \beta \rangle| = 9$ ). לכן,  $\langle \sigma_1, \sigma_2 \rangle$  מכילה תת חבורה בגודל 9. מצד שני,  $\sigma_1$  הוא מסדר 2 ולכן  $|\langle \sigma_1, \sigma_2 \rangle| = 9$ . מתחלק ב-18. לכן, בהכרח  $Gal(K/\mathbb{Q}) = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$  (ולמעשה,  $Gal(K/\mathbb{Q}) = \langle \sigma_1, \sigma_2 \rangle$ ).

הערה: דרך אחרת לבדוק ש- $Gal(K/\mathbb{Q}) = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$  היא להראות שבחבורת התמורות  $\langle (1,4)(2,6)(3,5), (1,4,2,6,3,5), (1,4,3,5,2,6) \rangle$  יש 10 תמורות שונות ולכן גודלה, שמתחלק ב-18, חייב להיות 18.

החבורה  $Gal(K/\mathbb{Q})$  לא אבלית כי  $\sigma_1\sigma_2 = \alpha \neq \beta = \sigma_2\sigma_1$ . מצד שני, היא לא איזומורפית ל- $D_9$  כי  $D_9$  מכילה איבר מסדר 9 ו- $Gal(K/\mathbb{Q})$  לא מכילה איבר מסדר 9 – זאת משום שהיא משוכנת ב- $S_6$  וב- $S_6$  אין איברים מסדר 9 (אין צורך להוכיח זאת בתרגיל).

**סעיף 3:** מתקיים  $\sigma_1 \left( \sqrt[3]{9 + \sqrt{-3}} + \sqrt[3]{9 - \sqrt{-3}} \right) = \sqrt[3]{9 + \sqrt{-3}} + \sqrt[3]{9 - \sqrt{-3}}$  ולכן לפי שאלה 2

$$K \neq \mathbb{Q} \left[ \sqrt[3]{9 + \sqrt{-3}} + \sqrt[3]{9 - \sqrt{-3}} \right]$$

**סעיף 4:** להלן פיתרון אחד מתוך הרבה אפשריים: אנו נשתמש באיברים  $\alpha, \beta$  שהוגדרו בסעיף 2.

נגדיר  $H = \langle a, b, s \mid a^3 = b^3 = s^2 = 1, ab = ba, as = sb \rangle$ . נראה כי  $H \cong Gal(K/\mathbb{Q})$ . נשים לב שכל איבר ב- $H$  ניתן לכתיבה בצורה  $s^i a^j b^k$  עם  $i \in \{0,1\}, j \in \{0,1,2\}, k \in \{0,1,2\}$  (הסבר: בכל ביטוי ב- $s, a, b$  ניתן להביא את ה- $s$ ים להיות השמאליים ביותר בעזרת היחסים). לכן,  $|H| \leq 18$ . מצד שני, קל לבדוק כי האיברים  $\sigma_1, \alpha, \beta$  מקיימים את היחסים שמקיימים  $s, a, b$  בהתאמה (בדקו!) ולכן קיים הומומורפיזם חבורות  $\psi: H \rightarrow Gal(K/\mathbb{Q})$  השולח את  $s, a, b$  אל  $\sigma_1, \alpha, \beta$  בהתאמה. היות ו- $Gal(K/\mathbb{Q})$  נוצרת ע"י  $\sigma_1, \alpha, \beta$  (הוכחנו בסעיף 2), נובע ש- $\psi$  על. אבל ב- $Gal(K/\mathbb{Q})$  יש 18 איברים ולכן בהכרח  $|H| \geq 18$ . לכן,  $|H| = 18$  ו- $\psi$  חייב להיות איזומורפיזם חבורות.