פתרון מטלה 08 — מבנים אלגבריים 2, 80446

10 ביוני 2025

שאלה 1

יהי K שדה עם p-rank של 1 (כלומר, $[K:K^p]=p^1$).

סעיף א'

נוכיח שלכל $n\in\mathbb{N}$, ל-K יש בדיוק הרחבה אחת L/K שהיא בלתי־ספרבילית לחלוטין (אי־פרידה בטהורה) מדרגה p^n וש־ $L=K\left(a^{\frac{1}{p^n}}\right)$ עבור כל $a\in K/K^p$.

הוכחה: נראה קודם קיום: מכך ש־ $[K:K^p]=p$, נובע ש־K הוא מרחב וקטורי ממימד 1 מעל K^p ולכן $K=K^p(a)$ (כי p ראשוני ולכן אין שדות ביניים בין K לבין K^p) עבור $a\in K\setminus K^p$.

נגדיר $L=K\left(a^{\frac{1}{p^n}}\right)$, $\alpha=a^{\frac{1}{p^n}}$ ואז $\alpha^{p^n}=a\in K$, אז $\alpha\in\overline{K}$ ולכן α הוא שורש של הפולינום $x^{p^n}-a$, נראה שהוא אי־פריק:

נניח שהוא פריק ב־$K[x]$ ולכן $a\in K^{p^m}$ עבור $m<n$ אבל אז $a\in K^p$ (במגדל ההרחבות יש לנו הכלה) וזו סתירה, ולכן הפולינום אי־פריק ומתקיים $[K(\alpha):K]=p^n$. ההרחבה הזאת אי־פרידה בטהרה: לפולינום $x^{p^n}-a$ יש רק שורש אחד (בגלל שהפרובניוס $x\mapsto x^p$ היא העתקה אי־פרידה גם בגלל $\gcd(f,f')=0$).

אז לפולינום הזה יש שורש יחיד והוא מהצורה $a^{\frac{1}{p^n}}$ אז עבור $\alpha=a^{\frac{1}{p^n}}$ נקבל $\alpha^{p^n}=a\in K$ אבל $\alpha^{p^k}\notin K$ לכל $k<n$ כי $a\notin K^p$, אז ההרחבה $L=K(\alpha)$ היא הרחבה אי־פרידה בטוהרה מדרגה p^n (זה מהתנאים השקולים גם לאי־פרידות בטהרה שראינו בהרצאה).

כעת, עלינו להראות יחידות: נניח כי L'/K היא הרחבה אי־פרידה בטהורה מדרגה p^n נוספת, ולכן קיים $\beta\in L'$ כך ש־$L=K(\beta)$ ומתקיים $\beta^{p^n}=b\in K$ וגם $x^{p^n}-b$ הוא פולינום אי־פריק מעל K, ולכן $L'=K\left(b^{\frac{1}{p^n}}\right)$ ונרצה להראות ש־$L=L'$:

מכך ש־ $[K:K^p]=p$ ו־$K=K^p(a)$ עבור $a\in K\setminus K^p$ נובע שכל $b\in K\setminus K^p$ ניתן לביטוי על־ידי $b=c^p\cdot a$ עבור $c\in K$, ומכיוון ש־ $a^{\frac{1}{p^n}}$, $b^{\frac{1}{p^n}}$ יוצרים הרחבות מדרגה p^n, בהכרח מתקיים

$$b^{\frac{1}{p^n}}=(c^pa)^{\frac{1}{p^n}}=c^{\frac{1}{p^{n-1}}}\cdot a^{\frac{1}{p^n}}$$

אבל $c\in K$ ולכן גם $c^{\frac{1}{p^{n-1}}}\in K$ וזה סוגר את היחידות.

$\square$

סעיף ב'

נוכיח שלכל הרחבה סופית L/K יש שדה ביניים $L/L_i/K$ כך ש־L_i/K היא בלתי־ספרבילית לחלוטין (אי־פרידה בטהורה) ו־L/L_i ספרבילית.

הוכחה: ראשית, מתקיים

$$K\subseteq K^{\frac{1}{p}}\subseteq K^{\frac{1}{p^2}}\subseteq\ldots\subseteq K^{\frac{1}{p^n}}$$

נבחר $L_i=L\cap K^{\frac{1}{p^\infty}}$ (משמע קיים $n\in\mathbb{N}$ כך שמתקיים $L_i=L\cap K^{\frac{1}{p^n}}$).

מסעיף א' אנחנו מקבלים $K^{\frac{1}{p^n}}=K\left(\alpha^{\frac{1}{p^n}}\right)$ עבור $\alpha\in K\setminus K^p$ ולכן $L_i=L\cap K\left(\alpha^{\frac{1}{p^n}}\right)$.

קודם כל, $L_i\subseteq K^{\frac{1}{p^n}}$ ולכן L_i/K הרחבה בלתי־ספרבילית לחלוטין לפי הטענה על תנאים שקולים שראינו בהרצאה.

נשאר להראת ש־L/L_i היא הרחבה ספרבילית, אבל נניח בשלילה שהיא לא ספרבילית: ולכן קיים $\alpha\in L$ כך שהפולינום המינימלי של α מעל L_i יש לו שורשים מרובים. מכיוון שאנחנו במציין p, הפולינום המינימלי של α הוא מהצורה

$$f(x)=(x-\alpha)^{p^k}g(x)$$

עבור $g(x)$ פולינום ש־α לא שורש שלו ו־$k\geq 1$.

אבל L_i היא אי־פרידה בטהרה מעל K ולכן כל איבר ב־L_i הוא שורש של פולינום מהצורה $x^{p^j}-a$ עבור $a\in K$.

היות ו־$\alpha\in L$ אבל $\alpha\notin L_i$, נבחן את הפולינום המינימלי של α מעל L_i. מההנחה, ההרחבה אי־פרידה בטוהרה ולכן הפולינום המינימלי של α מעל L_i הוא מהצורה

$$f(x)=(x-\alpha)^{p^k},\ k\geq 1$$

ולכן α הוא שורש של פולינום בלתי־ספרבילי לחלוטין מעל L_i.

אבל L_i נוצר על־ידי איברים עם חזקות p^m של $\alpha_1,\alpha_2,\ldots,\alpha_n$ ולכן האיברים ב־L_i הם מהצורה

$$\beta=c_1\alpha_1^{p^m}+c_2\alpha_2^{p^m}+\ldots c_n\alpha_n^{p^m}$$

עבור $c_i\in K$, אבל α_i הם לא חזקות p^m ב־L_i וזו סתירה להנחה (כי אחרת, אי אפשר לבנות את α לפי חזקות p^m אבל הנחנו שהפולינום בלתי־ספרבילי לחלוטין), ולכן קיבלנו סתירה ו־L/L_i הרחבה ספרבילית.

$\square$

שאלה 2

סעיף א'

נמצא תת־חבורה H מאינדקס 2 של $\mathrm{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ ונמצא במפורש אוטומורפיזם σ שיוצר אותה.

הוכחה: ראשית, מתקיים

$$2\mathbb{Z}/6\mathbb{Z} = \{0+6\mathbb{Z}, 2+6\mathbb{Z}, 4+6\mathbb{Z}\}$$

שנית,

$$[\mathbb{Q}(\xi_7):\mathbb{Q}] = \varphi_{\text{אוילר}}(7) = 6$$

וממה שראינו מתקיים

$$\mathrm{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q}) \simeq (\mathbb{Z}/7\mathbb{Z})^\times = \{1,2,34,5,6\} \Rightarrow \mathrm{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$$

אנחנו צריכים σ אוטומורפיזם בגלואה משמר את $\mathbb{Q}$ ועושה תמורה על שורשי היחידה הפרימיטיביים

$$\{\xi_7^1, \xi_7^2, \xi_7^3, \xi_7^4, \xi_7^5, \xi_7^6\}$$

אבל ξ_7 יוצר את כולם ולכן σ נקבע ביחידות לפי לאן הוא שולח את ξ_7 והוא כמובן נשלח לשורש יחידה אחר ξ_7^k עבור $k \in [6]$ ועליו לכבד כפליות

$$\sigma(\xi_7^m) = (\sigma(\xi_7))^m = \xi_7^{km}$$

אז $m \mapsto km \bmod 7 \in \mathrm{Aut}((\mathbb{Z}/7\mathbb{Z})^\times)$, וכפי שראינו זה בעצם $\mathrm{Aut}(\mathbb{Z}_6)$. עכשיו נגדיר $\sigma : \xi_7 \mapsto \xi_7^3$ ו־3 כי זה יוצר של $(\mathbb{Z}/7\mathbb{Z})^\times$

$$3^1 \underset{\bmod 7}{=} 3, 3^2 = 9 \underset{\bmod 7}{=} 2, 3^3 = 27 \underset{\bmod 7}{=} 6, 3^4 = 81 \underset{\bmod 7}{=} 4, 3^5 = 243 \underset{\bmod 7}{=} 5, 3^6 = 729 \underset{\bmod 7}{=} 1$$

ואז זה יוצר את כל החבורת גלואה. נשים לב שקיבלנו

$$\mathrm{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q}) = \langle\sigma\rangle \simeq \mathbb{Z}_6$$

אנחנו יודעים שתת־חבורה מאינדקס 2 היא חבורה מסדר 3, אז

$$H = \langle\sigma^2\rangle = \{\mathrm{id}, \sigma^2, \sigma^4\}$$

ו־H מכילה את האוטומורפיזמים

$$\xi_7 \mapsto \xi_7^{3^0} = \xi_7,\ \xi_7^{3^2} \mapsto \xi_7^2,\ \xi_7^{3^4} \mapsto \xi_7^4$$

$\square$

סעיף ב'

נחשב את $z = \sum_{h\in H} h(\xi_7)$ ונראה ש־$h(z) = z$ לכל $h \in H$.

הוכחה: ראשית, מתקיים מסעיף א'

$$z = \xi_7 + \xi_7^2 + \xi_7^4$$

ניקח $h \in H$, אז מתקיים

$$h(z) = h(\xi_7) + h(\xi_7^2) + h(\xi_7^4)$$

אבל ראינו שמתקיים בסעיף א' $h = \sigma_a \in H$ הנתונה על־ידי $h(\xi_7^k) = \xi_7^{ak} \bmod 7$ עבור $a \in \{1,2,4\}$.
עבור $a = 1$ ראינו, נשאר להראות עבור $a = 2, a = 4$:

$$\sigma_2(z) = \xi_7^2 + \xi_7^4 + \xi_7 = z$$
$$\sigma_3(z) = \xi_7^4 + \xi_7 + \xi_7^2 = z$$

ולכן לכל $h \in H$ מתקיים $h(z) = z$. $\square$

סעיף ג'

נסיך שמתקיים $z \in \mathbb{Q}(\xi_7)^H$ וש-$[\mathbb{Q}(z) : \mathbb{Q}] \leq 2$.

הוכחה: ראשית, $\mathbb{Q}(\xi_7)/\mathbb{Q}$ היא הרחבת גלואה וממה שראינו $H \leq \mathrm{Gal}(\mathbb{Q}(\xi_7)/\mathbb{Q})$ אז מהתזכורת גם מתקיים $\left[\mathbb{Q}(\xi_7)^H : \mathbb{Q}\right] = 2$.

מסעיף ב' נובע ישירות כי $z \in \mathbb{Q}(\xi_7)^H$ ולכן בהכרח גם מתקיים

$$[\mathbb{Q}(z) : \mathbb{Q}] \leq [\mathbb{Q}(\xi_7) : \mathbb{Q}] \leq 2$$

$\square$

סעיף ד'

נמצא $d \in \mathbb{Z}$ כך שמתקיים $\mathbb{Q}(z) = \mathbb{Q}\left(\sqrt{d}\right)$.

פתרון: עלינו להסתכל על החלק המרוכב ועל החלק הממשי כי אנחנו מחפשים $d \in \mathbb{Z}$.

נשים לב שהחלק הממשי של z מתקיים

$$\mathcal{R}(z) = \sum_{i=1}^{3} \cos\left(\frac{2^i \pi}{7}\right) = \cos\left(\frac{2\pi}{7}\right) + \cos\left(\frac{4\pi}{7}\right) + \cos\left(\frac{8\pi}{7}\right) = -\frac{1}{2}$$

אז

$$z = -\frac{1}{2} + i \cdot y \ (y \in \mathbb{R})$$

ולכן

$$z = \frac{-1 + i\sqrt{t}}{2}$$

עבור $t > 0$ כלשהו ואז נקבל $\mathbb{Q}(z) = \mathbb{Q}\left(\sqrt{t}\right)$.

נסתכל על המכפלה בצמוד ונחשב

$$z \cdot \overline{z} = \left(\xi_7 + \xi_7^2 + \xi_7^4\right) \cdot \left(\xi_7^{-1} + \xi_7^{-2} + \xi_7^{-4}\right) = \xi_7^0 + \xi_7^{-1} + \xi_7^{-3} + \xi_7 + \xi_7^0 + \xi_7^{-2} + \xi_7^3 + \xi_7^2 + \xi_7^0$$

$$\underset{\mathrm{mod}\, 7}{=} 3\xi_0^7 + \xi_7^6 + \xi_7^4 + \xi_7 + \xi_7^5 + \xi_7^3 + \xi_7^2 = 3 + \sum_{i=1}^{6} \xi_7^i \underset{\sum_{i=1}^{6} \xi_7^i = -1}{=} 3 - 1 = 2$$

ונשים לב שמזהויות המרוכבים מתקיים

$$z \cdot \overline{z} = 2 = |z|^2$$

וגם מתקיים

$$z + \overline{z} = \xi_7 + \xi_7^2 + \xi_7^4 + \xi_7^{-1} + \xi_7^{-2} + \xi_7^{-4} \underset{\mathrm{mod}\, 7}{=} \sum_{i=1}^{6} \xi_7^i = -1$$

אז מתקיים

$$z = -\frac{1}{2} + i \cdot \frac{\sqrt{t}}{2} \iff 2 = |z|^2 = \left|-\frac{1}{2} + i \cdot \frac{\sqrt{t}}{2}\right|^2 = \frac{1}{4} + \frac{t}{4} \iff 8 = 1 + t \iff t = 7$$

נבחר $d = 7$ ונקבל ש-$\mathbb{Q}(z) = \mathbb{Q}\left(\sqrt{d}\right)$. $\square$

שאלה 3

יהי K שדה, יהי $f \in K[x]$ פולינום אי־פריק וספרבילי ויהי L שדה פיצול של f מעל K.

סעיף א'

נוכיח שאם כל שדה ביניים $L/E/K$ הוא נורמלי אז כל שורש של f של f יוצר את L מעל K.

הוכחה: ראשית, $f \in K[x]$ פולינום אי־פריק וספרבילי ולכן בשדה פיצול יש $\alpha_1, ..., \alpha_n \in L$ שורשים שונים זה מזה ו־$L = K(\alpha_1, ..., \alpha_n)$ הרחבה סופית, ספרבילית ונורמלית ולכן הרחבת גלואה.

עלינו להראות שלכל שורש α מתקיים $L = K(\alpha)$.

היות ו־f אי־פריק וספרבילי מעל K ו־α הוא שורש של f, ההרחבה $E = K(\alpha) \subseteq L/K$ היא הרחבה ספרבילית עם דרגה r המקיימת $1 \leq r \leq \deg(f)$ ומההנחה גם נובע ש־$K \subseteq E \subseteq L/K$ היא נורמלית מעל K.

היות וההרחבה נורמלית, נובע שהפולינום מתפצל לחלוטין ב־$K(\alpha)$ ומכך ש־f אי־פריק מעל K ומתקיים $\alpha \in K(\alpha)$ ולכן כל שאר הצמודים נמצאים ב־$K(\alpha)$.

אבל f מתפצל לחלוטין ב־L (כי שדה פיצול) ואם f מתפצל ב־$K(\alpha)$ אז $K(\alpha)$ חייב להכיל את כל שאר השורשים של f, משמע $L = K(\alpha)$. $\square$

סעיף ב'

נסיק שאם $\mathrm{Gal}(L/K)$ אבלית אז כל שורש של f יוצר את L מעל K.

הוכחה: נניח כי $\mathrm{Gal}(L/K)$ אבלית ולכן כל $H \leq \mathrm{Gal}(L/K)$ היא נורמלית ב־$\mathrm{Gal}(L/K)$.

נסתכל על $L/E/K$, החבורה $\mathrm{Gal}(L/E) \leq \mathrm{Gal}(L/K)$ ולכן $\mathrm{Gal}(L/E)$ נורמלית ב־$\mathrm{Gal}(L/K)$.

לכן מתקיים ש־$E = L^{\mathrm{Gal}(L/K)}$ היא הרחבה נורמלית מעל K ולכן מסעיף א' נקבל שכל שורש של f יוצר את L מעל K. $\square$

שאלה 4

נסמן $f(x) = x^4 - 7x^2 + 7 \in \mathbb{Q}[x]$ ויהי L שדה פיצול של f.
נסמן β_1, β_2 שני השורשים של המשוואה $y^2 - 7y + 7 = 0$.

סעיף א'

נוכיח ש־$\mathbb{Q}(\beta_1, \beta_2) = \mathbb{Q}(\beta_1)$ ושמתקיים $\left[\mathbb{Q}\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right) : \mathbb{Q}(\beta_1)\right] = 4$.
הוכחה: השורשים של $y^2 - 7y + 7$ הם

$$y = \frac{7 \pm \sqrt{49 - 28}}{2} = \frac{7 \pm \sqrt{21}}{2}$$

נסמן בלי הגבלת הכלליות

$$\beta_1 = \frac{7 + \sqrt{21}}{2}, \ \beta_2 = \frac{7 - \sqrt{21}}{2}$$

נשים לב שמתקיים $\beta_2 = 7 - \beta_1$ כי

$$\beta_2 = \frac{7 - \sqrt{21}}{2} = 7 - \frac{7 + \sqrt{21}}{2} = \frac{14 - 7 - \sqrt{21}}{2} = \frac{7 - \sqrt{21}}{2}$$

ולכן בהכרח מתקיים $\mathbb{Q}(\beta_1, \beta_2) = \mathbb{Q}(\beta_1)$.
נשאר לחשב את $\left[\mathbb{Q}\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right) : \mathbb{Q}(\beta_1)\right]$.
במטלה 5 שאלה 3 סעיף ב' ראינו שמתקיים $\sqrt{\beta_2} \notin \mathbb{Q}\left(\sqrt{\beta_1}\right)$, ולכן בהכרח $\left[\mathbb{Q}\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right) : \mathbb{Q}\left(\sqrt{\beta_1}\right)\right] = 2$ כי הוספנו עוד איבר להרחבה.
מכפליות הדרגה נקבל

$$\left[\mathbb{Q}\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right) : \mathbb{Q}(\beta_1)\right] = \left[\mathbb{Q}\left(\sqrt{\beta_1}\right) : \mathbb{Q}(\beta_1)\right] \cdot \left[\mathbb{Q}\left(\sqrt{\beta_2}\right) : \mathbb{Q}\left(\sqrt{\beta_1}\right)\right] = 2 \cdot 2 = 4$$

□

סעיף ב'

נסיק ש־$L = \mathbb{Q}\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right)$ מדרגה 8 מעל $\mathbb{Q}$.
הוכחה: נשים לב ש־L היא הרחבה רדיקלית (נוצרת על ידי סיפוח של ביטוי שורשי לשדה הבסיס).
כמו־כן, במטלה 5 שאלה 3 סעיף ב' ראינו שההרחבה $\mathbb{Q}\left(\sqrt{\beta_1}\right)$ היא הרחבה מדרגה 4. מכפליות הדרגה וגם ממה שמצאנו בסעיף הקודם מתקיים

$$\left[\mathbb{Q}\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right) : \mathbb{Q}\left(\sqrt{\beta_1}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{\beta_1}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8$$

□

סעיף ג'

נמצא את טיפוס האיזומורפיזם של $\mathrm{Gal}(L/\mathbb{Q})$.
הוכחה: תהיי $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, מהגדרה אנחנו יודעים שמתקיים

$$\sigma\left(\sqrt{\beta_1}\right) \mapsto \pm\sqrt{\beta_1}$$
$$\sigma\left(\sqrt{\beta_2}\right) \mapsto \pm\sqrt{\beta_2}$$

בעצם יש לנו 8 אפשרויות שונות: זהות, שינוי סימן של אחד מהשורשים או שינוי סימן של שני השורשים (וכמובן יש גם שורש חיובי וגם שורש שלילי).
אז עלינו לחפש תתי־חבורות של S_4 (4 שורשים) מסדר 8.
חבורות מסדר 8 הן תת־חבורות 2־סילו של S_4, ממשפט סילו השלישי יש או 1 כזאת או 3 כאלו, אבל 1 לא אפשרית כי אז ממסקנה ממשפטי סילו היא תהיה תת־חבורה נורמלית של S_4 ואין ל־S_4 תת־חבורה נורמלית, ולכן יש 3 חבורות 2־סילו שהן צמודות זו לזו (ועל־כן איזומורפיות).
אפשר לספור את כמות החבורות מסדר 8 בידיים, כי היא חבורת־p סופית עבור $p = 2$, ולכן יש לה מרכז לא טריוויאלי והיא נילפוטנטית.
נוכל לסווג אותן לחבורות אבליות ולא אבליות:
עבור החבורות האבליות, משפט המיון לחבורות אבליות נוצרות סופית נותן אותן בשלמותן: $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$.

עבור החבורות הלא אבליות, אנחנו יודעים שהן D_4, Q_8 כאשר Q_8 היא חבורת הקווטרניונים.
ברור ש־$C_8 \not\subset S_4$ כי אין ב־S_4 איבר מסדר 8, וגם עבור $C_4 \times C_2 \not\subset S_4$ כי התתי־חבורות האבליות היחידות של S_4 היא חבורת קליין ו־$\mathbb{Z}_4$, ומאותה סיבה גם $C_2 \times C_2 \times C_2 \not\subset S_4$.
כמובן שגם $Q_8 \not\subset S_4$ מטעמי מבנה, ולכן נשאר לבחון רק את D_4:

$$D_4 = \langle r, s \mid r^4 = s^2 = e, srs = r^{-1} \rangle$$

אכן כמובן D_4 מסדר 8, ואנחנו יודעים שאפשר להסתכל על D_4 כסימטריות של המלבן, ואנחנו יודעים ש־D_4 פועלת על ארבעת קודקודי הריבוע בצורה נאמנה: נמספר את הקודקודים A, B, C, D ונסתכל על הפעולה של D_4 עליהם כאשר r סיבוב ב־90 מעלות ו־s שיקוף:

$$A \underset{r}{\mapsto} B,\ B \underset{r}{\mapsto} C,\ C \underset{r}{\mapsto} D,\ D \underset{r}{\mapsto} A$$
$$A \underset{r^2}{\mapsto} C,\ B \underset{r^2}{\mapsto} D,\ C \underset{r^2}{\mapsto} A,\ D \underset{r^2}{\mapsto} B$$
$$A \underset{r^2}{\mapsto} D,\ B \underset{r^3}{\mapsto} A,\ C \underset{r^3}{\mapsto} B,\ D \underset{r^3}{\mapsto} C$$
$$A \underset{s}{\mapsto} B,\ B \underset{s}{\mapsto} A,\ C \underset{s}{\mapsto} D,\ D \underset{s}{\mapsto} C$$
$$A \underset{sr}{\mapsto} C,\ B \underset{sr}{\mapsto} D,\ C \underset{sr}{\mapsto} A,\ D \underset{sr}{\mapsto} B$$
$$A \underset{sr^2}{\mapsto} D,\ B \underset{sr^2}{\mapsto} C,\ C \underset{sr^2}{\mapsto} B,\ D \underset{sr^2}{\mapsto} A$$
$$A \underset{sr^3}{\mapsto} B,\ B \underset{sr^3}{\mapsto} A,\ C \underset{sr^3}{\mapsto} D,\ D \underset{sr^3}{\mapsto} C$$

ולכן הפעולה היא נאמנה, ונשים לב שיצאה לנו פה תמורה ($A = 1, B = 2, C = 3, D = 4$) ולכן ניתן לשכן את D_4 לתת־חבורה של S_4 וכמובן מאותו סדר (8), ולכן קיבלנו שמתקיים $\mathrm{Gal}(L/\mathbb{Q}) \simeq D_4$.
ניקח $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, מתקיימים אחד מהבאים

$$\sigma\left(\sqrt{\beta_1}\right) \mapsto -\sqrt{\beta_1},\ \sigma\left(\sqrt{\beta_2}\right) \mapsto \sqrt{\beta_2}$$
$$\sigma\left(\sqrt{\beta_1}\right) \mapsto \sqrt{\beta_1},\ \sigma\left(\sqrt{\beta_2}\right) \mapsto -\sqrt{\beta_2}$$
$$\sigma\left(\sqrt{\beta_1}\right) \mapsto \sqrt{\beta_2},\ \sigma\left(\sqrt{\beta_2}\right) \mapsto \sqrt{\beta_1}$$

כאשר השניים הראשונים מקבילים ל־r והאחרון זה s. $\square$