מבנים אלגבריים 2, 80446 — פתרון מבחן מועד א׳ 2021

19 ביולי 2025

שאלה 1

בכל הרחבת שדות סופית וספרבילית L/K קיים איבר פרימיטיבי.

הוכחה: תחילה נוכיח למה:

למה 0.1 (משפט האיבר הפרימיטיבי חלק 1): תהיי L/K הרחבה סופית. אז L/K היא הרחבה פרימיטיבית אם ורק אם יש כמות סופית של שדות ביניים.

הוכחה: $\Longleftarrow$ תהיי L/K פרימיטיבית, כלומר $K=L(\alpha)$ ויהי F שדה ביניים. אז $f_{\alpha/F}=\sum_{i=1}^{n}a_it^i$.
יהי $L\subset F\subset E=K(a_0,\cdots,a_n)$ אז $f_{\alpha/F}\in E[t]$ ולכן $f_{\alpha/F}\mid f_{\alpha/E}$ ובפרט הם שווים.
לכן $[L:F]=\deg\left(f_{\alpha/F}\right)=\deg\left(f_{\alpha/E}\right)=[L:E]$ ולכן $E=F$ (כי $1=\frac{[L:E]}{[L:F]}=[F:E]$).
אז $F=K(a_1,\cdots,a_n)$ נקבע ביחידות על־ידי $f_{\alpha/F}$ ואנחנו יודעים ש־$f_{\alpha/K}\mid f_{\alpha/F}$ ולכן יש רק כמות סופית של אפשרויות ל־$f_{\alpha/F}$ (מקסימום $2^{[L:K]}=2^{\deg\left(f_{\alpha/K}\right)}$ כי $f_{\alpha/K}=\prod_{i=1}^{n}(t-\alpha_i)\in\overline{K}[t]$ ואם אני רוצה פולינום שיחלק, צריך לבחור קבוצה כלשהי של שורשים ויש 2^n אפשרויות לכל היותר).
$\Longrightarrow$ נניח שיש כמות סופית של שדות ביניים, $K\subset F_i\subset L$ עבור $1\leq i\leq m$.
אם K סופי, אז אנחנו יודעים ש־L/K פרימיטיבית , אז נניח ש־K אינסופי ונוכיח באינדוקציה על $[L:K]$:
הבסיס של דרגה 1 הוא טריוויאלי ולכן ניח שהטענה מתקיימת לכל הרחבה מדרגה הקטנה ל־$[L:K]$.
נכתוב $L=K(\alpha_1,\cdots,\alpha_r)$ הרחבה סופית וכן $E=K(\alpha_1,\cdots,\alpha_{r-1})$ (ואז $L=E(\alpha_r),\alpha=\alpha_r$).
נניח בלי הגבלת הכלליות ש־$L\neq E$ (אחרת נזרוק את α_r כי הוא מיותר).
מהנחת האינדוקציה, $E=K(\beta)$ כי ל־K יש רק מספר סופי של תתי־שדות.
ניקח סדרה אינסופית (מההנחה ש־K אינסופי) $c_1,c_2,\dots\in K$ וניקח $\gamma_i=\alpha+\beta c_i$ (צירופים לינאריים שונים של α,β).
נגדיר $F_j=K\left(\gamma_j\right)$ וקיימים $j\neq\ell$ כך ש־$F_j=F_\ell$ (כי יש כמות סופית של שדות ביניים וכמות אינסופית של איברים).
מתקיים $F_\ell=F_j\ni\frac{\gamma_\ell-\gamma_j}{c_\ell-c_j}=\frac{(\alpha+\beta c_\ell)-(\alpha+\beta c_j)}{c_\ell-c_j}=\beta$ ולכן $\alpha=\gamma_\ell-c_\ell\beta\in F_\ell$ ואז $\alpha,\beta\in F_j$, כלומר

$$L=K(\alpha,\beta)\subset F_j=K\left(\alpha+c_j\beta\right)=K\left(\gamma_j\right)$$

וזה בדיוק אומר ש־L/K פרימיטיבית. $\square$

אם כך, מספיק להוכיח שיש כמות סופית של שדות בינייםL נסתכל על סגור גלואה $L^{nor}=L^{\mathrm{gal}}/K$ (הסגור הנורמלי הוא סגור גלואה כי L/K פרידה) ומספיק להוכיח של־L^{gal}/K יש כמות סופית של שדות ביניים (כי $L\subset L^{\mathrm{gal}}$).
מהתאמת גלואה לכל $K\subset F\subset L^{\mathrm{gal}}$ מתקיים $F=L^{\mathrm{Gal}(L/F)}$ ולכן F נקבע ביחידות על־ידי $\mathrm{Gal}(L/F)\leq\mathrm{Gal}(L/K)$ ויש כמות סופית כזאת כי $\mathrm{Gal}(L/K)$ היא חבורה סופית. $\square$

שאלה 2

אם $n \in K^\times$ אז קיים שורש פרימיטיבי $\xi_n \in \overline{K}$ מסדר n, ההרחבה $K(\xi_n)/K$ היא גלואה וישנו שיכון $\mathrm{Gal}(K(\xi_n)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.

הוכחה: נניח ש-$n \in K^\times$, הפולינום $x^n - 1$ הוא ספרבילי ולכן ל-$\overline{K}$ יש n שורשי יחידה שונים.

ראינו שאם ל-$\overline{K}$ יש n שורשי יחידה שונים זה מזה, אז $\mu_n \cong (\mathbb{Z}/n\mathbb{Z})$, זו חבורה ציקלית ולכן יש לנו שורש יחידה פרימיטיבי ξ_n שיוצר אותה.

$K(\xi_n)/K$ הוא שדה הפיצול של הפולינום שלנו ולכן ההרחבה נורמלית וספרבילית ולכן זו הרחבת גלואה.

כל $\sigma \in G(L/K)$ נקבע ביחידות על־ידי $\sigma(\xi)$ ולכן אנחנו מקבלים שיכון $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(\mu_n)$ על־ידי $\sigma \mapsto \sigma|_{\mu_n}$.

נגדיר $\lambda : (\mathbb{Z}/n\mathbb{Z}) \to \mathrm{Aut}(\mu_n)$ על־ידי $a \mapsto \sigma_a$ כאשר $\sigma_a(\xi) = \xi^a$ לכל $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ והעתקה הזאת מגדירה את השיכון $\mathrm{Gal}(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$. $\square$

שאלה 3

בכל סעיף נקבע האם הטענה נכונה או לא נכונה וננמק לספורט.

סעיף א'

בחבורה $\mathrm{Aut}(\mathbb{F}_9)$ יש יותר איברים מאשר ב־$\mathrm{Aut}(\mathbb{F}_8)$.

הוכחה: הטענה **לא נכונה**.

נשים לב

$$\mathbb{F}_8 = \mathbb{F}_{2^3}, \mathbb{F}_9 = \mathbb{F}_{3^2}$$

ראינו שהשדות הסופיים $\mathbb{F}_q = \mathbb{F}_{p^n}$ עבור p ראשוני ו־$n \in \mathbb{N}$ הם יחידים עד־כדי איזומורפיזם, והאיברים בשדה $\mathbb{F}_{p^n}$ הם השורשים של הפולינום $x^{p^n} - x$.

ניזכר ש־$\mathrm{Aut}(\mathbb{F}_{p^n})$ נוצרת על־ידי אוטומורפיזם הפרובניוס ולכן $\mathrm{Aut}(\mathbb{F}_{p^n}) \cong \mathbb{Z}/n\mathbb{Z}$, ולכן ב־$\mathrm{Aut}(\mathbb{F}_8)$ יש יותר איברים. $\square$

סעיף ב'

תהיי L/K הרחבת שדות סופית ו־$\overline{L}$ סגור אלגברי של L. אם שני איברים $\alpha, \beta \in \overline{L}$ צמודים מעל L אז הם צמודים גם מעל K.

הוכחה: הטענה **נכונה**.

ניזכר $\overline{L}$ הוא סגור אלגברית, כלומר לכל פולינום ממעלה גדולה מ־1 יש שורש ב־$\overline{L}$. אם $\alpha, \beta \in \overline{K}$ צמודים, זה אומר שהם שורש של אותו פולינום (כי $\alpha \in \overline{K}$ אז הצמודים שלו מעל L הם השורשים של הפולינום המינימלי $f_{\alpha/L}$ ובאותו אופן גם על β).

אז $f_{\alpha/L} = f_{\beta/L}$, אבל $f_{\alpha/L} \mid f_{\alpha/K}$, ו־$f_{\alpha/K}$ הוא פולינום אי־פריק ומתוקן שגם β מאפס (כי אם β שורש של $f_{\alpha/L}$ הוא גם שורש של $f_{\alpha/K}$) וזה בידיוק אומר ש־$f_{\alpha/K} = f_{\beta/K}$ ולכן α, β צמודים מעל K. $\square$

סעיף ג'

תהיי E/K הרחבת שדות ויהיו L, F תתי־הרחבות כך ש־$E = LF$. אם E/F סופית אז L/K סופית.

הוכחה: הטענה **לא נכונה**.

גבע הראה את הטענה הזאת $\pm$ באחד התרגולים אבל הוא דיבר על איזומורפיזם כלשהו אבל הרעיון דומה: ניקח $K = \mathbb{F}_5, L = K(t), F = K(t^2)$, מתקיים $F \subseteq L$ ולכן מהגדרת הקומפוזיטום, $E = LF = L$ ומתקיים $[L : F] = 2$ בגלל הפולינום $x^2 - t^2$ שהוא פולינום אי־פריק אבל כמובן שמתקיים $[L : K] = \infty$ כי זה שדה הפונקציונליות הרציונליות עם t. $\square$

סעיף ד'

לכל חבורה סופית G יש הרחבת גלואה L/K כך שמתקיים $G \simeq \mathrm{Gal}(L/K)$.

הוכחה: הטענה **נכונה**.

משפט 0.1 (תזכורת: משפט קיילי): תהיי G חבורה סופית מסדר n. אז קיים שיכון (הומומורפיזם חד־חד ערכי) $\phi : G \to S_n$.

אז קיימת $H \leq S_n$ כך ש־$G \simeq H$.

נגדיר $L = \mathbb{Q}(t_1, \cdots, t_n)$ ו־$F = \mathbb{Q}(s_1, \cdots, s_n)$ כאשר $s_1, \cdots, s_n$ הם הפולינומים סימטריים.

ההרחבה L/F היא הרחבת גלואה כי אנחנו בשדה ממציין 0 ולכן כל פולינום אי־פריק הוא ספרבילי ואם t_i הוא שורש ב־L אז מהגדרת הפולינום הסימטריים אפשר לבטא אותו באמצעות פולינום סימטריים ולכן הוא מתפצל לחלוטין ב־L. אז מצאנו נורמליות + ספרבליות $\Longleftarrow$ גלואה.

בפרט מתקיים $\mathrm{Gal}(L/F) = S_n$ ו־H שדה שבת ולכן ממשפט ארטין $K^H = \{x \in K \mid \forall \sigma \in H \ \sigma(x) = x\}$ ולכן $\mathrm{Gal}(L/K) \simeq H \simeq G$.

$\square$

סעיף ה'

אם להרחבה סופית L/K אין תתי־הרחבות $K \subsetneq F \subsetneq L$ אז $[L : K]$ ראשוני.

הוכחה: לא יודעת, אבל התשובה **לא נכונה**.

$K = \mathbb{Q}(s_1, s_2, s_3, s_4), F = \mathbb{Q}(x_1, x_2, x_3, x_4)$ כאשר s_1, s_2, s_3, s_4 הפולינומים הסימטריים עם 4 משנים וראינו ש־L/F גלואה.

נסתכל על $H = S_3 \leq S_4$ ונסתכל על שדה השבת של H, $L = F^H$.

ממשפט ההתאמה, $[L : K] = \frac{|S_4|}{|S_3|} = 4$ ומצד שני אם הייתה תת־הרחבה $K \subsetneq F \subsetneq L$ כזאת אז מהמשפט היסודי של התאמת גלואה היה צריך להתקיים שיש התאמה ל־$S_3 \leq \mathscr{F}(F) \leq S_4$, אבל אין כזאת תת־חבורה ולכן אין כזה שדה. $\square$

שאלה 4

נתון פולינום אי־פריק $f(t)$ מעל $\mathbb{Q}$ ממעלה 3 עם חבורת גלואה ציקלית. נראה כי כל שורשי f ממשיים.

הוכחה: בגלל שהפולינום הוא אי־פריק מדרגה 3 אז כל α שהוא שורש של $f(t)$ מקיים $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$.

היות ול־$f(t)$ יש שלושה שורשים, שדה הפיצול מכיל את כולם והוא חייב להיות נורמלי ועל־כן גלואה מעל $\mathbb{Q}$, ולכן החבורת גלואה של ההרחבה צריכה להיות תת־חבורה של S_3 והתת־חבורה חייבת להיות טרנזטיבית ולכן זה או S_3 או C_3, אבל S_3 היא לא ציקלית (כי היא לא אבלית) ולכן אם K שדה הפיצול של הפולינום f אז $[K:\mathbb{Q}]=3$ ולכן חבורת הגלואה של ההרחבה היא C_3.

C_3 היא חבורה ציקלית מסדר אי־זוגי וכל האיברים הלא טריוויאלים שלה הם מסדר 3.

לו היה ל־f שורש מרוכב, אז להצמדה מרוכבת יש סדר 2 ול־C_3 אין איברים מסדר 2 ולכן לא יכול להיות לפולינום שורש מורכב ולכן כולם ממשיים.

כמה דברים שניסיתי בדרך: נשים לב שלפי פונקציית φ של אויילר, ל־C_3 יש בידיוק $\varphi_{\text{אויילר}}(3)=|\{n \mid 1\leq k\leq 3, \gcd(k,3)=1\}|=2$ יוצרים והם בידיוק $\{x^k \mid \gcd(k,3)=1\}=\{x,x^2\}$.

C_3 היא חבורה ציקלית מסדר אי־זוגי ולכן כל האיברים הלא טריוויאלים שלה הם מסדר 3 וראינו $\mathrm{Aut}(C_m)\cong\mathbb{Z}_m^\times$ ולכן

$$\mathrm{Aut}(C_3)\cong\mathbb{Z}_3^\times \Rightarrow |\mathrm{Aut}(C_3)|=2$$

זו כמובן גם חבורה ציקלית וכל אוטומורפיזם ϕ נקבע לפי לאן הוא שולח את היוצר σ, אז $\phi(\sigma)=\sigma^k, k\in\{1,2\}$. $\square$

שאלה 5

נמצא את הפירוק של $f(t)=t^8-1\in\mathbb{F}_{13}[t]$ לגורמים אי־פריקים.

פתרון: נשים לב שמתקיים

$$t^8-1=(t^4+1)(t^4-1)=(t^4+1)(t^2-1)(t^2+1)=(t^4+1)(t^2+1)(t-1)(t+1)$$

כמובן שמתקיים $x-12\underset{\bmod 13}{\equiv}x+1$.

צריך לבחון האם אפשר לפרק את הביטויים t^2+1,t^4+1 מעל $\mathbb{F}_{13}[t]$.

הערה (תזכורת – שימוש סמל לז'נדר):

הגדרה 0.1 (סמל לז'נדר): יהי p מספר ראשוני ($p\neq 2$) ו־$a\in\mathbb{Z}$, אז

$$\left(\frac{a}{p}\right)=\begin{cases}0 & a\equiv 0\pmod p\\ 1 & a\not\equiv 0\pmod p\wedge a\equiv x^2\pmod p\ \text{(}a\text{ זר ל־}p\text{ והוא שארית ריבועית מודלו }p\text{)}\\ -1 & a\not\equiv 0\pmod p\wedge a\not\equiv x^2\pmod p\ \text{(}a\text{ זר ל־}p\text{ ואינו שארית ריבועית מודלו }p\text{)}\end{cases}$$

למה 0.2: נניח ש־p ראשוני אי־זוגי.

1. כדי לבדוק אם לפולינום ריבועי ax^2+bx+c מעל שדה $\mathbb{F}_p$ יש פירוק, מספיק לבדוק אם סמל לז'נדר $\left(\frac{b^2-4ac}{p}\right)$ הוא 1 או -1.
אם הוא 1, זה אומר שיש ב־$\mathbb{F}_p$ שורש ל־b^2-4ac ואפשר להשתמש בנוסחת השורשים (שנותנת גם פירוק לפולינום מהצורה $a\cdot(x-r)\cdot(x-s)$ כאשר a המקדם המוביל ו־r,s השורשים).
2. כדי לבדוק עבור פולינום מהצורה x^2-c, מספיק לבדוק את סמל לז'נדר $\left(\frac{c}{p}\right)$ (שאומר לנו האם יש פיתרון למשוואה $x^2=c\pmod p$)

משפט 0.2 (משפט ההדדיות הריבועית): אם p,q ראשוניים אי־זוגיים, מתקיים

1.
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

2.
$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

3.
$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$

אם כך, עבור t^2+1 מתקיים

$$\left(-\frac{1}{13}\right)=(-1)^{\frac{13-1}{2}}=(-1)^6=1$$

ולכן יש לפולינום הזה פירוק (אם היה יוצא לנו -1, לא היינו צריכים לבדוק יותר).

בשלב הזה הבדיקה הופכת לידנית ועלינו לבחון לאילו $i\in\{0,\cdots,12\}$ מתקיים $i^2+1\underset{\bmod 13}{\equiv}0$ ובדיקה תביא לנו שזה קורה עבור $i\in\{5,8\}$, אז

$$t^2+1=(t-5)(t-8)\underset{\bmod 13}{\equiv}(t+8)(t+5)$$

נשאר לפרק את t^4+1, נגדיר $y=t^2$ ואז עם מה שמצאנו לעיל

$$t^4+1=y^2+1=(y+8)(y+5)=(t^2+8)(t^2+5)$$

אז רק נשאר להראות האם ל־$5,8$ יש שורשים ב־$\mathbb{F}_{13}$, אז לפי משפט ההדדיות הריבועית

$$\left(\frac{5}{13}\right)\left(\frac{13}{5}\right)=(-1)^{\frac{5-1}{2}\frac{13-1}{2}}=(-1)^{2\cdot 6}=(-1)^{12}=1$$

ולכן

$$\left(\frac{5}{13}\right)=\left(\frac{13}{5}\right)\cdot 1=\left(\frac{13}{5}\right)\underset{13\bmod 5=3}{\equiv}\left(\frac{3}{5}\right)$$

ואת $\left(\frac{3}{5}\right)$ יותר קל לנו לחשב ואחרי חישוב ידני נקבל שאין $n\in\mathbb{N}$ כך שמתקיים $n^2\underset{\bmod 5}{\equiv}3$ ולכן

$$\left(\frac{5}{13}\right)=\left(\frac{13}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=-1$$

ולכן לפולינום t^2-5 **אין פירוק מעל $\mathbb{F}_{\mathbf{13}}$**.

עבור הפולינום t^2-8, נשים לב ש־$t^2+5 = \underset{\bmod 13}{\equiv} t^2-8$ אז נוכל להשתמש במה שמצאנו ועם (2) ממשפט ההדדיות הריבועית ולראות שמתקיים

$$\left(-\frac{5}{13}\right)=\left(-\frac{1}{13}\right)\cdot\left(\frac{5}{13}\right)=(-1)^{\frac{13-1}{2}}\cdot -1=(-1)^{12}\cdot(-1)=(-1)$$

ולכם גם לפולינום t^2-8 **אין פירוק מעל $\mathbb{F}_{\mathbf{13}}$**.

תשובה סופית

$$t^8-1=(t^4+1)(t^2+1)(t-1)(t+1)=(t-1)(t-12)(t-8)(t-5)(t^2-8)(t^2-5\text{ש})$$

$\square$

שאלה 6

יהיו $p,q,r\in\mathbb{Q}[x,y,z]$ הפולינומים $p=x+y+z, q=xy+yz+xz, r=xyz$.

הערה: אלו הפולינומים הסימטריים s_1,s_2,s_3 בהתאמה.

סעיף א'

נבטא את $x^2y^2+y^2z^2+z^2x^2$ כפולינום $P(p,q,r)$ ב־p,q,r.

פתרון: נתחיל מלחשב

$$\begin{aligned}q^2=(xy+yz+xz)(xy+yz+xz)&=x^2y^2+xy^2z+x^2yz+y^2zx+y^2z^2+yz^2x+x^2zy+xyz^2+x^2z^2\\&=x^2y^2+y^2z^2+x^2z^2+2(x^2yz+y^2xz+z^3xy)\end{aligned}$$

אז

$$\begin{aligned}x^2y^2+y^2z^2+z^2x^2-q^2&=\cancel{x^2y^2}+\cancel{y^2z^2}+\cancel{z^2x^2}-\cancel{x^2y^2}-\cancel{y^2z^2}-\cancel{z^2x^2}-2(x^2yz+y^2xz+z^3xy)\\&=-2(x^2zy+y^2zx+z^2xy)\end{aligned}$$

נשים לב שמתקיים

$$x^2zy+y^2zx+z^2xy=(xyz)(x+y+z)=rp$$

ולכן

$$x^2y^2+y^2z^2+z^2x^2=q^2+rp$$

□

סעיף ב'

נמצא את הפולינום המינימלי $f_\alpha(t)\in K[t]$ של האיבר $\alpha=x^2y+y^2z+z^2x\in\mathbb{Q}(x,y,z)$ מעל $K=\mathbb{Q}(p,q,r)$.

פתרון: לא יודעת. □

שאלה 7

נמצא את $\mathrm{Gal}(K^{nor}/\mathbb{Q})$ בכל סעיף עבור K נתון.

הערה (תזכורת – K^{nor}): אם L/K הרחבה אלגברית, אז **הסגור הנורמלי** של L/K, שמסומן לפעמים כ־L^{nor}, הוא ההרחבה הנורמלית של K הקטנה ביותר כך ש־$L^{nor}/L/K$.

סעיף א'

$K = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$.

פתרון: נסמן $\alpha = \sqrt{1+\sqrt{2}}$, אז

$$\alpha^2 = 1+\sqrt{2} \iff \alpha^2 - 1 = \sqrt{2} \iff \left(\alpha^2-1\right)^2 = 2 \iff \alpha^4 - 2\alpha^2 + 1 = 2 \iff \alpha^4 - 2\alpha^2 - 1 = 0$$

נשים לב שהפולינום $x^4 - 2x^2 - 1$ הוא אי־פריק (אפשר לפי האלגוריתם שראינו במטלה 2 לראות שאין לו שורשים).
נשים לב שעבור $b=-2, c=-1$ מתקיים $(b^2-4c)c = (4+4)\cdot(-1) = -8 \notin \mathbb{Q}^2$.
אז $\sqrt{1+\sqrt{2}}$ הוא כמובן שורש, אבל נשים לב שגם $\sqrt{1-\sqrt{2}}$ הוא שורש, כי

$$\left(\sqrt{1-\sqrt{2}}\right)^4 - 2\left(\sqrt{1-\sqrt{2}}\right)^2 - 1 = 1 - 2\sqrt{2} + 2 - 2\left(1-\sqrt{2}\right) - 1 = 0$$

וגם נשים לב שמכך ש־$\sqrt{2} = \alpha^2 - 1$ ומכך ש־$\sqrt{2} \notin \mathbb{Q}$, אפשר לכתוב את $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{1+\sqrt{2}}\right)$.
בנוסף, לפולינום $\alpha^2 - \left(1+\sqrt{2}\right) = 0$ יש שורש $\pm\sqrt{1+\sqrt{2}}$ וגם לפולינום $x^2 - 2 = 0$ יש שורש $\pm\sqrt{2}$.
מצאנו את כל השורשים של הפולינום המינימלי $(x^4 - 2x^2 - 1)$ ולכן $K^{nor} = \mathbb{Q}\left(\sqrt{2}, \sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}\right)$.
זה דומה למה שעשינו בתרגיל בית 8 שאלה 4 אז נעבוד דומה ולכן $[K^{nor} : \mathbb{Q}] = 8$ וזו כמובן הרחבה נורמלית וספרבילית ולכן הרחבת גלואה.
יש לנו 4 שורשים אז עלינו לחפש תתי־חבורות של S_4 מסדר 8 ואנחנו יודעים שיש 5 חבורות מסדר 8

$$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_4, Q_8$$

נשים לב שמכולן רק D_4 פועלת טרנזיטיבית על ארבעה איברים והפעולה של D_4 היא נאמנה, יש לה איברים מסדר 4 ו־2 וכל השורשים שלנו הם צמודים אחד של השני ולכן מבחינת מבנה D_4 מתאימה.
(באופן כללי, Q_8 לא תת־חבורה של S_4 ולכן נפסלת ול־S_4 אין איבר מסדר 8 ולכן C_8 לא אופציה וגם תתי־החבורות האבליות היחידות של S_4 הן $\mathbb{Z}_4$ וחבורת קליין אז גם $C_2 \times C_2 \times C_2, C_4 \times C_2$ נפסלו ונשארנו עם D_4). $\square$

סעיף ב'

$K = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$.

פתרון: נסמן $\alpha = \sqrt{2+\sqrt{2}}$ אז

$$\alpha^2 = 2+\sqrt{2} \iff \alpha^2 - 2 = \sqrt{2} \iff \alpha^4 - 4\alpha^2 + 4 = 2 \iff \alpha^4 - 4\alpha^2 + 2 = 0$$

נשים לב שהפולינום $f(x) = x^4 - 4x^2 + 2$ הוא פולינום אי־פריק בבחירה של $p=2$ מקריטריון אייזנשטיין אבל אם נסמן $b=-4, c=2$ נקבל $(b^2-4c)c = (16-8)\cdot 2 = 16 \in \mathbb{Q}^2$ ואז לפי התרגול לכאורה יש דרך קיצור. $\square$