פתרון מטלה 05 — מבנים אלגבריים 2, 80446

17 במאי 2025

שאלה 1

סעיף א'

נוכיח שחבורה אבלית סופית היא מכפלה ישרה של חבורות הסילו שלה.
נסיק שאם $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ פירוק לחזקות של ראשוניים שונים אז $\mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}} \simeq \mathbb{Z}_n$ ושהאיזומורפיזם הזה שולח את הקבוצה

$$\left\{(x_1, ..., x_r) \mid \ \forall 1 \leq i \leq r, \ \langle x_i \rangle = \mathbb{Z}_{p_i^{k_i}}\right\} \mapsto \{x \in \mathbb{Z}_n \mid \langle x \rangle = \mathbb{Z}_n\}$$

הוכחה: נסמן $|A| = n = p_1^{a_1} \cdot ... \cdot p_k^{a_k}$ עבור $p_1, ..., p_k$ שונים זה מזה.
ממשפט סילו הראשון נובע שקיימות תתי־חבורות $A_{p_1}, ..., A_{p_k}$ כל אחת מסדר p_i מתאים, וממשפט לגראנז' נובע שלכל $i \neq j \in [k]$ מתקיים $A_{p_i} \cap A_{p_j} = \{e\}$, ולכן מתאמי סדר נקבל

$$A = A_{p_1} \times A_{p_2} \times ... \times A_{p_k}$$

ונגדיר $\varphi : A_{p_1} \times A_{p_2} \times ... \times A_{p_k} \to A$ על־ידי $\varphi(a_1, ..., a_k) = a_1 \cdot ... \cdot a_k$.
היות ו־A אבלית, נובע שהמכפלה $a_1 \cdot ... \cdot a_k$ לא תלויה בסדר המכפלה ומכאן נובע ישר כי φ הוא הומומורפיזם.
נניח כי $\varphi(a_1, ..., a_k) = e$ ולכן $a_1 \cdot ... \cdot a_k = e$, היות וכל איבר במכפלה הוא מסדר p_i מתאים (ששונים זה מזה מההנחה) ונקבל שכל $a_i = e$.
אם נניח בשלילה כי $a_1 \neq e$, נקבל $a_1 = (a_2 \cdot ... \cdot a_k)^{-1}$, אבל $p_1 \nmid o(a_2 \cdot ... \cdot a_k)^{-1}$ בגלל שזו מכפלה של איברים מסדר שהוא זר ל־p_1 וזו סתירה, ולכן $a_1 = ... = a_k = e$ משמע $\ker(\varphi) = e$ ולכן φ חד־חד ערכית.
φ על, כי אם ניקח $a \in A$ והוא יהיה בידיוק ב־A_{p_i} יחיד ולכן בלי הגבלת הכלליות נניח כי $a \in A_{p_1}$ ונוכל לבחור $\varphi(a, e, ..., e) = a$.
לכן φ איזומורפיזם וקיבלנו ש־A איזומורפית למכפלה של החבורות סילו שלה.
עבור ההסקה, נבחין שזה נובע ממשפט השאריות הסיני: היות ו־$n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ ראשוניים שונים זה מזה נובע כי לכל $i \neq j \in [r]$ מתקיים $\gcd\left(p_i^{k_i}, p_j^{k_j}\right) = 1$ וזאת גם בידיוק המכפלה של החבורות סילו מההוכחה לעיל וממשפט השאריות הסיני נקבל ש־

$$\mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}} \simeq \mathbb{Z}_n$$

הנתון על־ידי $\varphi : \mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}} \to \mathbb{Z}_n$, ואיזומורפיזם מכבד את מבנה החבורה ולכן שולח יוצרים ליוצרים ולכן היוצרים של $\mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}}$ נשלחים ליוצרים של $\mathbb{Z}_n$.

□

סעיף ב'

נוכיח ש־$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ ובנוסף שאם $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ פירוק לחזקת ראשוניים שונים אז

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right)^\times \times ... \times \left(\mathbb{Z}/p_r^{k_r}\mathbb{Z}\right)^\times$$

הוכחה: ראשית, 1 יוצר את $\mathbb{Z}/n\mathbb{Z}$ ולכן להגדיר את $f \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ זה כמו להגדיר את $f(1)$.
f היא חד־חד ערכית ועל כי חייב להתקיים $o(f(1)) = n$ וממבנים1 אנחנו כבר יודעים שזה שקול לכך ש־$\gcd(f(1), n) = 1$.
אם $g \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ אז

$$g \circ f(1) = g(f(1)) = g\left(\underbrace{1 + ... + 1}_{f(1)\text{ פעמים}}\right) = \underbrace{g(1) + ... + g(1)}_{f(1)\text{ פעמים}} = g(1)f(1)$$

משמע $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ איזומורפית לחבורה שאיבריה הם המספרים הטבעיים הקטנים מ־n וזרים לו עם פעולת הכפל, וזה בידיוק $(\mathbb{Z}/n\mathbb{Z})^\times$.
נניח ש־$n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ פירוק לחזקת ראשוניים שונים ולכן מהסעיף הקודם

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Aut}\left(\mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}}\right) \simeq \mathrm{Aut}\left(\mathbb{Z}_{p_1^{k_1}}\right) \times ... \times \mathrm{Aut}\left(\mathbb{Z}_{p_r^{k_r}}\right)$$

ויחד עם מה שהראינו מתקיים

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \Rightarrow (\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Aut}\left(\mathbb{Z}_{p_1^{k_1}}\right) \times ... \times \mathrm{Aut}\left(\mathbb{Z}_{p_r^{k_r}}\right) \simeq \left(\mathbb{Z}_{p_1^{k_1}}\right)^\times \times ... \times \left(\mathbb{Z}_{p_r^{k_r}}\right)^\times$$

□

סעיף ג'

תהיי $(A, +)$ חבורה אבלית סופית. נסיק מסעיף א' שאם לכל p ראשוני כך ש־$p \mid |A|$ מתקיים ש־$A[p] = \{a \in A \mid \exists k \in \mathbb{N}\ s.t.\ p^k a = 0\}$ ציקלית אז A ציקלית.

הוכחה: היות ו־A חבורה אבלית סופית נובע שהיא מכפלה ישרה של החבורות סילו שלה, ולכן

$$A \cong \mathbb{Z}_{p^{k_1}} \times ... \times \mathbb{Z}_{p^{k_m}}$$

עבור $k_1 + ... + k_m = n$ ונבחן את

$$A[p] = \{a \in A \mid \exists k \in \mathbb{N}\ s.t.\ p^k a = 0\}$$

ולכן מהגדרה נובע שכל חבורת p_i סילו של A מוכלת ב־$A[p]$ ולכן $p_i^{k_i} \mid |A[p]|$.

מההנחה כי $A[p]$ ציקלית, נובע שקיים $a \in A[p]$ מסדר $p_i^{k_i}$ ולכן $\langle a \rangle$ היא חבורת סילו של A שהיא ציקלית.

זה נכון לכל $p_i^{k_i}$ במכפלה, ולכן נקבל ש־A היא מכפלה ישרה של חבורות ציקליות מסדרים שונים ובמקרה זה נקבל ש־A ציקלית: נראה רק למקרה של מכפלה של 2 חבורות ציקליות מסדרים שונים, והמקרה הפרטי הזה מספיק להוכחה של כל מכפלה ישרה סופית: נניח שיש לנו C_n, C_m שתי חבורות ציקליות מסדרים זרים ואנחנו יודעים ש־$C_n \times C_m = \{(x, y) \mid x \in C_n, y \in C_m\}$.

נניח ש־$C_n \times C_m$ לא ציקלית, ולכן לכל $x \in C_n \times C_m$ מתקיים $o(x) < nm$, ולכן $\mathrm{lcm}(n, m) < nm$ וזה בהכרח גורר ש־$\gcd(n, m) > 1$, אבל הנחנו שהסדרים זרים זה לזה ולכן $\gcd(n, m) = 1$ וזאת סתירה, ולכן מכפלה ישרה של חבורות ציקליות מסדרים זרים היא ציקלית ומאינדוקציה נקבל ש־A ציקלית. $\square$

סעיף ד'

נוכיח שאם $(A, +)$ אבלית מסדר p^n ל־p ראשוני כלשהו ובנוסף ל־A יש תת־חבורה ציקלית יחידה מסדר p אז A ציקלית.

הוכחה: אם $n = 1$ אז הטענה טריוויאלית, ולכן נניח ש־$n > 1$.

מסעיף א' נסיק שמתקיים $A \cong \mathbb{Z}_{p^{k_1}} \times ... \times \mathbb{Z}_{p^{k_m}}$ עבור $k_1 + ... + k_m = n$. נגדיר

$$A[p] := \{x \in A \mid px = e\}$$

תת־חבורת פיתול של האיברים מסדר המחלק את p, וזה מרחב וקטורי מעל $\mathbb{F}_p$ שמימדו הוא $\dim_{\mathbb{F}_p} A[p] = k$, כי במילים אחרות תת־חבורת הפיתול היא המכפלה הישרה של כל $\mathbb{Z}/p^{a_i}\mathbb{Z}$.

נטען כעת שאם המימד גדול מ־2 אז יש שתי תתי־חבורות מסדר p שהן ממימד 1 (חבורה ציקלית היא תת־מרחב מדרגה 1), ואז

$$\left(p^k - 1\right)(p - 1) \geq \frac{p^2 - 1}{p - 1} = p + 1 > 1$$

ולכן יש ל־A לפחות שתי תתי־חבורות מסדר p וזו סתירה להנחה.

אז A היא מכפלה ישרה של תת־חבורה אחת מסדר p שהיא ציקלית, ולכן A ציקלית.

נניח בשלילה כי A לא ציקלית, ולכן בהכרח יש לפחות שני גורמים במכפלה הישרה לעיל שמצאנו $\square$

סעיף ה'

ננסח ונוכיח חיזוק של סעיף ג' באמצעות הטענה מסעיף ד'.

הוכחה: ניסוח: אם $(A, +)$ חבורה אבלית כל שלכל $p \mid |A|$ עבור p ראשוני מתקיים ש־$A[p]$ אבלית עם תת־חבורה ציקלית יחידה מסדר p, אז A ציקלית.

הוכחה: מסעיף ד' אנחנו מקבלים ש־$A[p]$ ציקלית לכל $p \mid |A|$ ראשוני, ומסעיף ג' נקבל ש־A ציקלית (שכן החבורות סילו של A הן ציקליות ולכן A ציקלית בתור מכפלה ישרה של חבורות ציקליות מסדרים זרים). $\square$

שאלה 2

סעיף א'

נראה שאם $\varepsilon_1,\dots,\varepsilon_n\in\{\pm 1\}$ אז יש אוטומורפיזם של $\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$ ששולח את $\sqrt{p_i}$ ל-$\varepsilon_i\sqrt{p_i}$, לכל i.

הוכחה: עבור בסיס האינדוקציה: עבור $n=1$, נסמן $K=\mathbb{Q}[x]/(x^2-p_1)$ ונגדיר שני איזומורפיזמים $\varphi_1,\varphi_2:K\to\mathbb{Q}\left(\sqrt{p_1}\right)$ על־ידי

$$\varphi_2\left(\overline{f}\right)=f(\varepsilon_1\sqrt{p_1}),\ \ \varphi_1\left(\overline{f}\right)=f(\sqrt{p_1})$$

דהיינו φ_1,φ_2 הם הצמדה וזהות שאנחנו כבר יודעים שהם איזומורפיזמים, ונגדיר $\alpha:\mathbb{Q}\left(\sqrt{p_1}\right)\to\mathbb{Q}\left(\sqrt{p_1}\right)$ על־ידי $\alpha=\varphi_2\circ\varphi_1^{-1}$ ונקבל

$$\alpha(\sqrt{p_1})=\varphi_2(\varphi_1^{-1}(\sqrt{p_1}))=\varphi_2\left(\overline{f}(x)\right)=\varepsilon_1\sqrt{p_1}$$

נסמן $L=\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{n-1}}\right)$ ונניח שראינו את נכונות הטענה עבור מקרה זה ונראה עבור $\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_{n-1}},\sqrt{p_n}\right)$.

במטלה 3 ראינו שמתקיים $\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right):\mathbb{Q}\right]=2^n$, ולכן $\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)=\frac{L\left(\sqrt{p_n}\right)}{L[x]}/(x^2-p_n)$ ונגדיר שני איזומורפיזמים $\varphi_1,\varphi_2:\frac{L[x]}{x^2-p_n}\to\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$ על־ידי

$$\varphi_1\left(\overline{f}\right)=f(\sqrt{p_b}),\ \ \varphi_2\left(\overline{f}\right)=\varphi_2(c_0+c_1\overline{x}+\dots+c_n\overline{x_n}^n)=\alpha(c_0)+\alpha(c_1)\varepsilon_1\sqrt{p_1}+\dots\alpha(c_n)\varepsilon_n\sqrt{p_n}$$

נגדיר $\beta:\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)\to\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$ על־ידי $\beta=\varphi_2\circ\varphi_1^{-1}$ כמקודם, וזה מביא לנו אוטומורפיזם.

$\square$

סעיף ב'

נראה שאם $\varepsilon_1,\dots,\varepsilon_n\in\{\pm 1\}$ אז $\sum_{i=1}^n\varepsilon_i\sqrt{p_i}$ צמוד של $\sum_{i=1}^n\sqrt{p_i}$מעל $\mathbb{Q}$ ונסיק שיש להם את אותו הפולינום המינימלי מעל $\mathbb{Q}$.

הוכחה: מהסעיף הקודם אנחנו יודעים שיש אוטומורפיזם σ של $\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$ שמקיים

$$\sigma\left(\sum_{i=1}^n\sqrt{p_i}\right)=\sum_{i=1}^n\sigma\left(\sqrt{p_i}\right)=\sum_{i=1}^n\varepsilon_i\sqrt{p_i}=\beta$$

נסתכל על $\sigma\mid_{\mathbb{Q}(\alpha)}:\mathbb{Q}(\alpha)\to\mathbb{Q}(\beta)$: בהרצאה ראינו ששני איברים הם צמודים מעל שדה אם ורק אם הם שורשים של אותו פולינום אי־פריק ופולינום מינימלי הוא כמובן אי־פריק ולכן יש להם בפרט את אותו פולינום מינימלי מעל $\mathbb{Q}$.

$\square$

סעיף ג'

נחשב את דרגת הפולינום המינימלי של $\sqrt{p_1}+\dots+\sqrt{p_n}$ מעל $\mathbb{Q}$ ונסיק שאם $p_1,\dots,p_n$ ראשוניים שונים זה מזה אז

$$\mathbb{Q}(\sqrt{p_1}+\dots+\sqrt{p_n})=\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$$

הוכחה: נסמן $f=\sqrt{p_1}+\dots+\sqrt{p_n}$.

מהסעיפים הקודמים אנחנו יודעים של-f יש 2^n שורשים שונים שהם $f=\varepsilon_1\sqrt{p_1}+\dots+\varepsilon_n\sqrt{p_n}$ ולכן $\deg(f)\ge 2^n$.

אבל זה פולינום מינימלי, והדרגה של הפולינום המינימלי קטנה או שווה לדרגת ההרחבה, ולכן נובע ש-$\deg_{\mathbb{Q}}(f)\le 2^n$ (כי $\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right):\mathbb{Q}\right]=2^n$) ולכן $\deg_{\mathbb{Q}}(f)=2^n$.

אז נקבל ש-$\left[\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right):\mathbb{Q}\left(\sqrt{p_1}+\dots+\sqrt{p_n}\right)\right]=1$ ולכן $\mathbb{Q}\left(\sqrt{p_1}+\dots\sqrt{p_n}\right)=\mathbb{Q}\left(\sqrt{p_1},\dots,\sqrt{p_n}\right)$.

$\square$

שאלה 3

בכל סעיף נתון $f \in \mathbb{Q}[x]$, נוכיח ש־f אי־פריק ובנוסף עבור $\alpha \in \mathbb{C}$ שורש שרירותי של f נגדיר את $K = \mathbb{Q}(\alpha)$ ונקבע האם K/A הרחבה נורמלית.

סעיף א'

$f(x) = x^4 + x^3 + x^2 + x + 1$.

הוכחה: ראשית נשים לב שבהרצאה ראינו ש־$\phi_5 = x^4 + x^3 + x^2 + x + 1$ וזהו פולינום ציקלוטומי ולכן $f(x) = \phi_5 = \frac{x^5-1}{x-1}$ ובמטלה 3 ראינו כבר שהוא אי־פריק עבור $p = 3, n = 1$.

כעת, השורשים של f מעל $\mathbb{C}$ הם $\left\{e^{\frac{2\pi i n}{5}} \mid 1 \le n \le 4\right\}$.

בלי הגבלת הכלליות נבחר $\omega = \alpha$. למה מותר לנו לעשות את זה? אנחנו יודעים ש־f הוא הפולינום המינימלי של $\mathbb{Q}\left(\omega^k\right)$ לכל $k \in [4]$ מהיותו שורש, משמע $\left[\mathbb{Q}\left(\omega^k\right) : \mathbb{Q}\right] = \deg(f) = 4$ ונראה ש־$\mathbb{Q}\left(\omega^k\right) = \mathbb{Q}(\omega)$:

ההכלה הראשונה $\mathbb{Q}\left(\omega^k\right) \subseteq \mathbb{Q}(\omega)$ היא ישירות מהגדרה, ההכלה בכיוון השני $\mathbb{Q}(\omega) \subseteq \mathbb{Q}\left(\omega^k\right)$ נובע מכך ש־$\gcd(k, 5) = 1$ ולכן קיים $m \in \mathbb{Z}$ כך שיתקיים $km \equiv 1 \bmod 5$ ולכן $\left(\omega^k\right)^m = \omega^{km} = \omega$ וקיבלנו את ההכלה בכיוון השני.

לכן, $\mathbb{Q}(\alpha) = \mathbb{Q}(\omega)$ מכיל את כל השורשים של f ולכן f מתפצל לחלוטין ב־$\mathbb{Q}(\alpha)$ וזה מקיים את התנאים השקולים לנורמליות שראינו בהרצאה (אי־פריק מעל $\mathbb{Q}[x]$, יש לו שורש ב־$\mathbb{Q}(\alpha)$ והוא מתפצל לחלוטין מעל $\mathbb{Q}(\alpha)$). $\square$

סעיף ב'

$f(x) = x^4 - 7x^2 + 7$.

הוכחה: ראשית, מקריטריון אייזנשטיין אנחנו יודעים ש־f הוא אי־פריק עבור $p = 7$, נסמן $t = x^2$ ולכן $p(t) = x^2 - 7t + 7$ ואז השורשים של $p(t)$ הם

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

והשורשים של f הם

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

נראה שההרחבה לא נורמלית: נפעל לפי הרמז וניקח $\beta_1 = \alpha^2$ אחד השורשים שמקיים $\beta^2 - 7b + 7 = 0$ ולמשוואה $y^2 - 7y + 7 = 0$ שני פיתרונות, β_1, β_2.

בלי הגבלת הכלליות, נבחר $\beta_1 = \frac{7+\sqrt{21}}{2} = \alpha$ ונניח בשלילה ש־$\sqrt{\beta_2} \in \mathbb{Q}\left(\sqrt{\frac{7+\sqrt{21}}{2}}\right)$ וראינו שזו הרחבה מדרגה 4 ולכן

$$\mathcal{B} = \left\{1, \alpha, \sqrt{21}, \alpha\sqrt{21}\right\}$$

מהווה בסיס להרחבה $\mathbb{Q}(\alpha)$ ונשים לב ש־$\beta_1, \beta_2 \in \mathbb{Q}\left(\sqrt{21}\right)$ ו־$\{1, \alpha\} \subseteq \mathcal{B}$ מהווה בסיס ל־$\mathbb{Q}(\alpha)/\mathbb{Q}\left(\sqrt{21}\right)$ $(\star)$ ו־$\left[\mathbb{Q}\left(\sqrt{21}\right) : \mathbb{Q}\right] = 2$, ולכן גם מתקיים $\mathbb{Q}\left(\sqrt{21}\right) \subseteq \mathbb{Q}(\alpha)$. מההנחה קיימים $a, b, c, d \in \mathbb{Q}$ כך שמתקיים

$$\sqrt{\beta_2} = a + b\alpha + c\sqrt{21} + d\alpha\sqrt{21} \iff \beta = \left(\left(a + c\sqrt{21}\right) + \left(b + \sqrt{21}d\right)\alpha\right)^2$$

$$\underset{\alpha^2=\beta_1}{=} \left(a + c\sqrt{21}\right)^2 + \beta_1\left(b + \sqrt{21}d\right)^2 + 2\left(a + c\sqrt{21}\right)\left(\alpha\left(b + \sqrt{21}d\right)\right)$$

נשים לב שמתקיים

$$(\diamond)\ \beta_1\beta_2 = \left(\frac{7+\sqrt{21}}{2}\right)\left(\frac{7-\sqrt{21}}{2}\right) = \frac{\left(7+\sqrt{21}\right)\left(7-\sqrt{21}\right)}{4} = \frac{49-21}{4} = 7$$

$$(\diamond\diamond)\ \beta_1 + \beta_2 = \left(7 + \sqrt{21} + 7 - \sqrt{21}\right) = \frac{14}{2} = 7$$

מ־$(\star)$ נקבל שחייב שיתקיים $2\left(a+c\sqrt{21}\right)\left(b+\sqrt{21}d\right)=0$ שכן $\alpha\neq 0$, ונחלק למקרים:

1. אם $a+c\sqrt{21}=0$.

$$\beta_2=\beta_1\left(b+\sqrt{21}d\right)^2\iff\beta_2^2=\beta_1\beta_2\left(b+\sqrt{21}d\right)^2\underset{\diamond}{\iff}\beta_2^2=7\left(b+\sqrt{21}d\right)^2$$

$$\iff\frac{49-14\sqrt{21}+21}{4}=7\left(b+\sqrt{21}d\right)^2\iff 7(\beta_2-1)=7\left(b+\sqrt{21}d\right)^2$$

$$\Rightarrow\beta_2-1=\left(b+\sqrt{21}d\right)^2\iff\frac{5-\sqrt{21}}{2}=b^2+2db\sqrt{21}+21d^2$$

ולכן צריך להתקיים

$$b^2+21d^2=\frac{5}{2},\ 2bd=-\frac{1}{2}\iff bd=-\frac{1}{4}$$

נכפול את הביטוי הראשון ב־b^2 ונקבל עם הביטוי הראשון ש־$b^2d^2=-\frac{1}{16}$

$$b^4+21d^2b^2=\frac{5}{2}b^2\iff b^4+\frac{21}{14}=\frac{5}{2}b^2\iff\left(b^2-\frac{7}{4}\right)\left(b^2-\frac{3}{4}\right)=0$$

אבל לא קיים אף $b\in\mathbb{Q}$ כך ש־$b^2=\frac{3}{4}$ או ש־$b^2=\frac{7}{4}$ וזה מקרה לא אפשרי.

2. אם $b+d\sqrt{21}=0$ אז מתקיים

$$\beta_2=\left(a+c\sqrt{21}\right)^2=a^2+21c^2+2ac\sqrt{21}$$

ולכן צריך להתקיים

$$a^2+21c^2=\frac{7}{2},\ 2ac=-\frac{1}{2}\iff ac=-\frac{1}{4}$$

שוב נכפול ב־a^2 ונקבל ממה שראינו $a^2c^2=-\frac{1}{16}$ ואז

$$a^4+21c^2a^2=\frac{7}{2}a^2\iff a^4+\frac{21}{16}=\frac{7}{2}a^2\iff a^4-\frac{7}{2}a^2+\frac{21}{16}$$

וגם במקרה הזה אין פיתרון מעל $\mathbb{Q}$.

בשני המקרים מצאנו שלא ייתכן ש־$\sqrt{\beta_2}\in\mathbb{Q}(\alpha)$ ולכן זו סתירה ובאותו אופן נקבל עבור $\alpha=\beta_2$ ולכן $\mathbb{Q}(\alpha)$ לא מכילה את כל השורשים ולכן $\mathbb{Q}(\alpha)/\mathbb{Q}$ לא הרחבה נורמלית. $\square$

סעיף ג'

$f(x)=x^4-x-1$.

הוכחה: נעזר ברמז, עבור אי־פריקות נראה שזה אי־פריק מודלו 2:

נראה תחילה שהפולינום x^2+x+1 הוא הפולינום הריבועי האי־פריק היחידי מעל $\mathbb{F}_2$: ראשית, כל הפולינומים ממעלה 2 הם:

1. $x^2+0x+0=x^2$
2. $x^2+1x+0=x^2+x$
3. $x^2+0x+1=x^2+1$
4. $x^2+1x+1=x^2+x+1$

נבחן אי־פריקות לכל אחד בהתאמה:

1. הוא אי־פריק כ־$x\cdot x$
2. נבחן קודם כל לפי שורשים
   1. $x=0$ ואז $0^2+1=1\neq 0$ ולכן לא שורש
   2. $x=1$ ואז $1^2+1=2\bmod 2=0$ ולכן 1 הוא שורש ואנחנו כבר יודעים שהפיצול שלו הוא

$$x^2+x=(x+1)(x+1)=x^2+2x+1\underset{\bmod 2}{=}x^2+1$$

משמע בין כה וכה הפולינום הוא פריק.

3. $x^2+x=x(x+1)$ ולכן פריק

4. נבחן קודם כל לפי שורשים

1. $x=0$ ואז $0^2+0+=1$ ולכן לא שורש
2. $x=1$ ואז $1 \underset{\bmod 2}{=} 1^2+1+1$ ולכן לא שורש

לכן אין לפולינום x^2+x+1 שורשים ב־$\mathbb{F}_2$ ולכן הוא אי־פריק לפי טענה מתרגיל 1.

עכשיו נשים לב

$$x^4-x-1 \underset{\bmod 2}{=} x^4+x+1$$

ולפולינום x^4+x+1 אין שורשים מעל $\mathbb{F}_2$ (כי $0 \neq 1 = 1+0+0^4, 0 \neq 1 \underset{\bmod 1}{=} 1+1+1^4$) ולכן $f_{\bmod 2}$ לא מתפרק לגורמים לינאריים מעל $\mathbb{F}_2$ ונרצה להראות שהוא לא מתפרק לפי חזקות ריבועיות: נניח בשלילה שהוא כן, אז קיימים $a,b,c,d \in \mathbb{F}_2$ כן שמתקיים

$$x^4+x+1=(x^2+ax+b)(x^2+cx+d)=x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd$$

אבל חישוב ישיר יראה לנו שהפיתרון היחידי למערכת זה $b=d=1, a=c=0$ אבל $x^4+1=x^4+2x^2+1 \neq x^4+x+1$ ולכן f אי־פריק מעל $\mathbb{F}_2$ (מספיק להוכיח שהוא אי־פריק מעל $\mathbb{F}_2$ כי ראינו שאם פולינום הוא פריק ב־$\mathbb{Q}[x]$ הוא גם בהכרח פריק מעל $\mathbb{F}_p[x]$ עבור p ראשוני).
עבור הנורמליות, נמצא כמה שורשים ממשיים יש עבור f: נשים לב ש־$f'=4x^3-1$ ולכן יש נקודת מינימום יחידה. נשים לב שגם מתקיים

$$f(x) \xrightarrow[x\to\infty]{} \infty, f(x) \xrightarrow[x\to-\infty]{} \infty$$

לכן ממשפט ערך הביניים נקבל שיש שני שורשים ממשיים, אבל אנחנו יודעים שיש לו גם שורשים מרוכבים: לכן אם נבחר α שורש שרירותי של f נקבל ש־f לא מתפצל לחלוטין מעל $\mathbb{Q}(\alpha)/\mathbb{Q}$ ולכן ההרחבה לא נורמלית. $\square$

שאלה 4

יהי K שדה שבו החבורה μ_∞ מתפצלת (כלומר, לכל שורש יחידה $z \in \overline{K}$ מתקיים $z \in K$). נסמן $p = \mathrm{char}(K)$ אם המציין של K חיובי ואחרת $p = 1$ ונראה שמתקיים $\mu_\infty(K) \cong \mathbb{Q}/\left(\mathbb{Z}\left[\frac{1}{p}\right]\right)$.

הוכחה: נחלק לנוחות לשני מקרים

1. $\mathrm{char}(K) = 0$ ולכן $p = 1$.

   K סגור אלגברית ולכן מכיל את כל שורשי היחידה ξ_n לכל n. כל $\frac{a}{n} \in \mathbb{Q}/\mathbb{Z}$ הוא מסדר סופי ולכן $\mathbb{Q}/\mathbb{Z}$ היא חבורת פיתול עם "עותק" לכל $\mathbb{Z}/n\mathbb{Z}$ לכל $n \geq 1$, וזה בידיוק $\mu_\infty(K)$: נסתכל על ההומומורפיזם $\varphi : \mathbb{Q}/\mathbb{Z} \to \mu_\infty(K)$ הנתון על־ידי $\varphi\left(\frac{p}{q} + \mathbb{Z}\right) = e^{\frac{2\pi i p}{q}}$, נראה שזה איזומורפיזם וזה יסיים:

   1. מוגדר היטב כי אם $\frac{p}{q} \equiv \frac{p'}{q'} \bmod \mathbb{Z}$ אז

   $$\frac{p}{q} - \frac{p'}{q'} \in \mathbb{Z} \Rightarrow e^{2\pi i \frac{p}{q}} = e^{2\pi i \frac{p'}{q'}} \cdot e^{2\pi i \left(\frac{p}{q} - \frac{p'}{q'}\right)} = e^{2\pi i \frac{p'}{q'}} \cdot 1 = e^{2\pi i \frac{p'}{q'}}$$

   2. אכן הומומורפיזם

   $$\varphi\left(\left(\frac{p}{q} + \mathbb{Z}\right) + \left(\frac{p'}{q'} + \mathbb{Z}\right)\right) = \varphi\left(\left(\frac{p}{q} + \frac{p'}{q'}\right) + \mathbb{Z}\right) = e^{2\pi i \left(\frac{p}{q} + \frac{p'}{q'}\right)} = e^{2\pi i \frac{p}{q}} \cdot e^{2\pi i \frac{p'}{q'}} = \varphi\left(\frac{p}{q} + \mathbb{Z}\right) \cdot \varphi\left(\frac{p'}{q'} + \mathbb{Z}\right)$$

   3. חד־חד ערכי

   $$\varphi\left(\frac{p}{q} + \mathbb{Z}\right) = 1 \iff e^{2\pi i \frac{p}{q}} = 1 \iff \frac{p}{q} \in \mathbb{Z} \Rightarrow \frac{p}{q} + \mathbb{Z} = 0 + \mathbb{Z}$$

   4. על כי כל $\xi \in \mu_\infty(\mathbb{C})$ הוא שורש יחידה, ולכן הוא מהצורה $\xi = e^{2\pi i \frac{p}{q}}$ ולכן $\varphi\left(\frac{p}{q} + \mathbb{Z}\right) = \xi$.

2. במקרה השני, $\mathrm{char}(K) = p > 1$.

   יהי $\xi \in K$ שורש יחידה מסדר p^n, משמע $\xi^{p^n} = 1$ ולכן ξ הוא שורש של $x^{p^n} - 1$, אבל $\left(x^{p^n} - 1\right)' = 0$ כי $\mathrm{char}(K) = p$ ולכן $\gcd\left(x^{p^n} - 1, \left(x^{p^n} - 1\right)'\right) = 1$ ולכן זהו פולינום פריד.

   מנגד, כל השורשי יחידה במציין p חייבים להיות מסדר זר ל־p, ולכן

   $$\mu_\infty(K) = \bigcup_{\substack{n \geq 1, \\ \gcd(n,p)=1}} \mu_n(K)$$

   אבל זה בידיוק אומר ש־$\mu_{\infty(K)} \cong \mathbb{Q}/\mathbb{Z}\left[\frac{1}{p}\right]$, שכן כל $x \in \mathbb{Q}/\mathbb{Z}$ הוא מהצורה $x = \frac{a}{n} + \mathbb{Z}$, ואם $p \mid n$ אז $\xi_n \notin K$, ולכן נשאר רק עם n־ים שעבורם $\gcd(n,p) = 1$, משמע

   $$\mu_\infty(K) \cong \biguplus_{\substack{n \geq 1, \\ \gcd(n,p)=1}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z}\left[\frac{1}{p}\right]$$

□