פתרון מטלה 01 — מבנים אלגבריים 2, 80446

27 במרץ 2025

שאלה 1

תהיי L/K הרחבת שדות כך ש־$[L:K]=7$. נראה שלכל איבר $\alpha\in L\setminus K$ מתקיים $L=K[\alpha]$.

הוכחה: יהי $\alpha\in L\setminus K$ ונבחן את ההרחבה $K[a]/K$.

ניזכר שמהגדרה $K[\alpha]=\{f(\alpha)\mid f\in K[\alpha]\}$ הוא תת־החוג הקטן ביותר של L שמכיל את α ו־

נבחן את $[K[\alpha]:K]$ וניזכר כי זה שקול למימד של $K[\alpha]$ מעל K.

בהרצאה ראינו את היחס בין שרשרת ההכלות לבין דרגת ההרחבות המתאימה: $[K[\alpha]:K]\cdot[L:K[\alpha]]=[L:K]\underset{\text{נתון}}{=}7$.

7 ראשוני ולכן נקבל כי $[K[\alpha]:K]=1$ או $[K[\alpha]:K]=7$.

נשים לב כי לא יתכן שיתקיים $[K[\alpha]:K]=1$ שכן מהגדרת הדרגה של ההרחבה היה נובע כי $K[\alpha]=K$ אבל הנחנו כי $\alpha\notin K$.

נסיק כי מתקיים $[K[\alpha]:K]=7$.

נשים לב שמתקיים כעת:

$$[L:K[\alpha]]=1\Longleftarrow[L:K[\alpha]]\cdot 7=[L:K[\alpha]]\cdot[K[\alpha]:K]=[L:K]\underset{\text{נתון}}{=}7$$

זאת אומרת, L הוא מרחב וקטורי ממימד 1 מעל $K[\alpha]$ ולכן קיבלנו $L=K[\alpha]$ $\square$

שאלה 2

יהי $\mathbb{F}$ שדה סופי. נראה שיש $p \in \mathbb{N}$ ראשוני ו־$n \in \mathbb{N}$ כך ש־$|\mathbb{F}| = p^n$.

הוכחה: ראשית מהיות $\mathbb{F}$ שדה נובע כי הוא תחום שלמות ולכן אין בו מחלקי אפס לא טריוויאלים.
נסמן $p = \mathrm{char}(\mathbb{F})$ ונתחיל מלהראות שהמציין של שדה הוא או אפס או מספר ראשוני:
נניח בשלילה ש־p לא מספר ראשוני ולכן $p = \alpha \cdot \beta$ כך שמתקיים $0 < \alpha, \beta < p$.
מהגדרת המציין נובע:

$$0_{\mathbb{F}} = \underbrace{1 + ... + 1}_{\text{p times}} = \underbrace{\underbrace{1 + ... + 1}_{\alpha \text{ times}} + ... + \underbrace{1 + ... + 1}_{\alpha \text{ times}}}_{\beta \text{ times}}$$

מהסגירות נובע $\lambda = \underbrace{1 + ... + 1}_{\alpha \text{ times}} \in \mathbb{F}$.
נשים לב כי $\lambda \neq 0_{\mathbb{F}}$ שכן ממינימליות p ומהיות $\alpha < p = \mathrm{char}(\mathbb{F})$ נקבל סתירה ולכן $\lambda \neq 0_{\mathbb{F}}$.
כעת מהיות $\mathbb{F}$ שדה נובע שקיים $\lambda^{-1} \in \mathbb{F}$ כך שמתקיים:

$$0_{\mathbb{F}} = 0_{\mathbb{F}} \cdot \lambda^{-1} = \left(\underbrace{\lambda + ... + \lambda}_{\beta \text{ times}} \right) \cdot \lambda^{-1} = \underbrace{1 + ... + 1}_{\beta \text{ times}}$$

אבל אז $\mathrm{char}(\mathbb{F}) = \beta > p$ וזו סתירה למינימליות p.
לכן p ראשוני או 0, אבל מהיות $\mathbb{F}$ שדה סופי נובע מעיקרון שובך היונים כי $p \neq 0$.
כעת, לכל איבר ב־$\mathbb{F}$ יש סדר p בחבורה החיבורית $(\mathbb{F}, +)$ ולכן $(\mathbb{F}, +)$ היא חבורת־p:
יהי $x \in \mathbb{F} \neq 0_{\mathbb{F}}$, מתקיים: $p \cdot x = p \cdot (1_{\mathbb{F}} \cdot x) \underset{(1)}{=} (p \cdot 1_{\mathbb{F}}) \cdot x = 0_{\mathbb{F}}$ כאשר (1) נובע מדיסטריבוטיביות החוג ולכן $(\mathbb{F}, +)$ היא חבורת־p.
ראינו כי חבורה היא חבורת־p אם ורק אם היא מסדר p^n עבור p ראשוני ו־$n \in \mathbb{N}$ וקיבלנו את הנדרש. $\square$

שאלה 3

TBD

סעיף א'

הוכחה: $\square$

סעיף ב'

הוכחה: $\square$

שאלה 4

יהי $\mathbb{F}$ שדה ויהי $f \in \mathbb{F}[x]$.

סעיף א'

נראה שאם $\deg(f) = 1$ אז f ראשוני.

הוכחה: ניזכר כי $\mathbb{F}[x]$ הוא תחום שלמות המקיים את שרשרת הגרירות הבאה: תחום אוקלידי $\Longleftarrow$ תחום ראשי $\Longleftarrow$ תחום פריקות יחידה.
נניח כי $\deg(f) = 1$ אבל f לא ראשוני ולכן הוא פריק ואז קיימים $g, h \in \mathbb{F}[x]$ כך שמתקיים $g \cdot h = f$.
ניזכר שמתכונות פונקציית הדרגה נובע $\deg(p \cdot q) = \deg(p) + \deg(q)$ לכל $p, q \in \mathbb{F}[x]$.
במקרה שלנו מתקיים: $1 = \deg(f) = \deg(g \cdot h) = \deg(g) + \deg(h)$ אבל לכל $p \in \mathbb{F}[x]$ מתקיים $0 \leq \deg(p) \in \mathbb{N}$ ולכן או שמתקיים $\deg(g) = 0 \wedge \deg(h) = 1$ או שמתקיים $\deg(g) = 1 \wedge \deg(h) = 0$.
בלי הגבלת הכלליות נניח שמתקיים $\deg(g) = 1 \wedge \deg(h) = 0$ ולכן נובע כי $h \in \mathbb{F}$ אבל פולינום ממעלה 0 בשדה הוא הפיך ולכן קיבלנו מהגדרה כי f הוא אי־פריק (מבוטא על־ידי מכפלה עם הפיך).
אבל בתחום ראשי ובתחום פריקות יחידה ראשוני $\Longleftrightarrow$ אי־פריק וקיבלנו את הנדרש. $\square$

סעיף ב'

נוכיח שאם $\deg(f) = 2$ או $\deg(f) = 3$ אז f ראשוני אם ורק אם $f(\alpha) \neq 0$ לכל $\alpha \in \mathbb{F}$.

הוכחה:
$\Longleftarrow$ נניח ש־f ראשוני ונרצה להראות שלכל $\alpha \in \mathbb{F}$ מתקיים $f(\alpha) \neq 0$.
מהיות f ראשוני בדומה לסעיף א' נובע כי הוא אי־פריק ולכן הוא לא מתפרק לגורמים לינאריים, כלומר אין לו שורשים (גם ראינו במבנים1).
לכן אם בשלילה נניח כי קיים $\alpha \in \mathbb{F}$ כך ש־$f(\alpha) = 0$ ינבע כי $x - \alpha$ הוא פקטור ב־$f(x)$ ולכן יהיה אפשר לחלק את $f(x)$ ב־$x - \alpha$ אבל f הוא אי־פריק מההנחה וזו סתירה.
$\Longrightarrow$ נניח שלכל $\alpha \in \mathbb{F}$ מתקיים $f(\alpha) \neq 0$ ונרצה להראות ש־f ראשוני.
מההנחה נובע כי ל־f אין שורשים ב־$\mathbb{F}$, זאת אומרת שאי אפשר לפרק את f למכפלה $f = (x - \alpha)g(x)$ כאשר $\alpha \in \mathbb{F}, g(x) \in \mathbb{F}[x]$.
אבל f הוא מדרגה 2 או 3, ולכן כל פירוק שלו בהכרח יכיל פקטור לינארי של $x - \alpha$, אבל ל־f אין אף שורש כזה ולכן נקבל כי f הוא אי־פריק ובהתאם לסעיף א' הוא ראשוני. $\square$

סעיף ג'

נראה הכי הטענה מסעיף ב' לא מתקיימת כאשר $\deg(f) \geq 4$.

הוכחה: נסתכל על הפולינום $\mathbb{Q}[x] \ni f(x) = x^4 - 2x^1 + 1$.
זהו פולינום שאנחנו כבר יודעים שיש לו שורש שהוא $x = \pm 1$ שכן $f(1) = 0, f(-1) = 0$.
אבל מתקיים:

$$f(x) = x^4 + 2x^1 + 1 = (x^2 - 1)(x^2 - 1)$$

כאשר האחרון הוא כמובן פולינום לא פריק מעל $\mathbb{Q}[x]$ כי אין לו אפילו פיתרון.
מנגד, נסתכל על הפולינום $\mathbb{Q}[x] \ni q(x) = x^4 + 1$.
כפי שאנחנו יודעים אין לפולינום זה שורשים מעל $\mathbb{Q}[x]$ שכן הפיתרון לפולינום זה הוא $x^4 = -1$ אבל מתקיים

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

אז ראינו שלפולינום מדרגה 4 יכול להיות ללא שורשים אך פריק , ויכול להיות עם שורשים ולהיות אי־פריק והטענה מסעיף ב' לא נכונה בהכרח. $\square$

שאלה 5

נסמן $\mathbb{E}=\mathbb{Q}[x]/(x^3-5)$.

סעיף א'

נראה ש־$\mathbb{E}$ שדה ושהוא איזומורפי לתת־השדה המינימלי של $\mathbb{R}$ שמכיל את $\sqrt[3]{5}$.

הוכחה: ראינו (במבנים1) שלכל שדה $\mathbb{F}$ חוג הפולינומים $\mathbb{F}[x]$ הוא תחום אוקלידי ולכן $\mathbb{Q}[x]$ תחום אוקלידי וכמו בשאלה 4 משרשרת הגרירות נובע כי $\mathbb{Q}[x]$ תחום ראשי ותחום פריקות יחידה ובתחומים אלו ראשוני $\iff$ אי־פריק.
נסמן $\mathbb{Q}[x] \trianglerighteq f=x^3-5\neq 0$ וניזכר כי המנה $\mathbb{E}=\mathbb{Q}[X]/(f)$ היא שדה אם ורק אם f אידיאל מקסימלי. אז נראה ש־f אידיאל מקסימלי.
נשים לב שמשאלה 4 נובע כי f הוא פולינום ראשוני:
f מדרגה 3 ולכל $\alpha\in\mathbb{Q}$ מתקיים $f(\alpha)\neq 0$ שכן $f(\alpha)=0\iff\alpha=\sqrt[3]{5}$ ואין לכך פיתרון לאף $\alpha\in\mathbb{Q}$.
נראה שאין פיתרון כזה:
נניח שכן, ולכן $\sqrt[3]{5}=\frac{p}{q}$ עבור $p\in\mathbb{Z},q\in\mathbb{N}$ כשבר מצומצם, ולכן היה מתקיים $5q^3=p^3$ ולכן $5\mid p$ (5 הוא ראשוני ומחלק של p^3).
נסמן $p=5k$ עבור $k\in\mathbb{N}$ ולכן $5q^3=(5k)^3=125k^3\iff q^3=25k^3$ ולכן באותו אופן נקבל כי q מתחלק ב־5.
אבל הנחנו ש־$\frac{p}{q}$ הוא שבר מצומצם ולכן זו סתירה ומשאלה 4 נקבל כי f ראשוני ועל כן אי־פריק.
ניזכר כי בתחום ראשי R מתקיים לכל $R\trianglerighteq(\pi)\neq 0$ שרשרת הגרירות הבאה: (π) ראשוני $\iff$ π ראשוני $\iff$ π אי־פריק $\iff$ (π) מקסימלי.
ולכן קיבלנו כי f אידיאל מקסימלי והמטענה מהתרגול מתקיים כי $\mathbb{E}=\mathbb{Q}[X]/(f)$ שדה.
TBD לחלק השני. $\square$

סעיף ב'

הוכחה: $\square$

שאלה 6

TBD בונוס

סעיף א'

הוכחה: □

סעיף ב'

הוכחה: □

סעיף ג'

הוכחה: □