פתרון מטלה 01 — מבנים אלגבריים 2, 80446

28 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 K ו־α.

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

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:

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

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 $x \in \mathbb{F}$,$x \neq 0_{\mathbb{F}}$, 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: □

סעיף ב'

הוכחה: □

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 $g(x) \in \mathbb{F}[x], \alpha \in \mathbb{F}$.
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 שהטענה מסעיף ב' לא מתקיימת כאשר $\deg(f) \geq 4$.

הוכחה: נסתכל על הפולינום $x^4 - 2x^1 + 1 = f(x) \in \mathbb{Q}[x]$.
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 $x^4 + 1 = q(x) \in \mathbb{Q}[x]$.
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 שפולינום 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 $\Longleftrightarrow$ 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 $\alpha=\sqrt[3]{5}\Longleftrightarrow f(\alpha)=0$ 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 $5q^3=(5k)^3=125k^3\Longleftrightarrow q^3=25k^3$ 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 $\Longleftrightarrow$ π ראשוני $\Longleftrightarrow$ π אי־פריק $\Longleftrightarrow$ (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

יהי $\mathbb{F}$ שדה סופי ונסמן $q=|\mathbb{F}|$.
נגיד כי פולינום $f(x)=\sum_{i=0}^n a_ix^i\in\mathbb{F}[x]$ הוא מתוקן אם $a_n=1$.

סעיף א'

נוכיח שב־$\mathbb{F}[x]$ יש $q+\binom{q}{2}$ פולינומים מתוקנים פריקים מדרגה 2.

הוכחה: פולינום מתוקן מדרגה 2 הוא מהצורה $f(x)=x^2+bx+c\in\mathbb{F}[x]$ עבור $a,b\in\mathbb{F}$ ונראה שפולינום מתוקן הוא פריק אם ורק אם הוא מהצורה $(x-a)(x-b)=(x-b)(x-a)$ עבור $a,b\in\mathbb{F}$ או מהצורה $(x-a)^2$ עבור $a\in\mathbb{F}$: יהי $0\neq\in\mathbb{F}[x]$ פולינום מתוקן.

$\Longleftarrow$ נניח ש־f פריק ונראה שהוא מהצורה $f=(x-a)(x-b)=(x-b)(x-a)$ עבור $a,b\in\mathbb{F}$ או מהצורה $f=(x-a)^2$ עבור $a\in\mathbb{F}$.
כמקודם, אנחנו יודעים ש־$\mathbb{F}[x]$ הוא תחום פריקות יחידה ובתחום פריקות יחידה, ראשוני $\iff$ אי־פריק.
מההנחה כי f פריק נובע שקיימים $p_1,...,p_n\in\mathbb{F}[x]$ אי־פריקים לאו דווקא שונים זה מזה כך שמתקיים $f=p_1p_2\cdots p_n$.
אבל אנחנו יודעים שלפולינום ממעלה n יש לכל היותר n שורשים ב־$\mathbb{F}$ (ראינו במבנים1 וההוכחה נובעת באינדוקציה על מעלת פולינום) ולכן במקרה שלנו $1\le n\le 2$ שכן הנחנו כי הפולינום פריק ואנחנו יודעים ש־$a\in\mathbb{F}$ הוא שורש של הפולינום f אם ורק אם $(x-a)\mid f\in\mathbb{F}[x]$.
לכן אם יש לו שורש אחד $a\in\mathbb{F}$ נקבל כי $f=(x-a)^2$ ואם יש לו שני שורשים $a,b\in\mathbb{F}$ נקבל כי $f=(x-a)(x-b)\underset{(1)}{=}(x-b)(x-a)$ כאשר (1) נובע מהיות החוג קומוטטיבי.
$\Longrightarrow$ נניח כי f מהצורה $f=(x-a)(x-b)=(x-b)(x-a)$ עבור $a,b\in\mathbb{F}$ או מהצורה $f=(x-a)^2$ עבור $a\in\mathbb{F}$ ונראה ש־f פריק.
נשים לב כי הפולינומים $(x-a),(x-b)$ הם מדרגה 1 ולכן לפני שאלה 4 הם ראשוניים ובפרט מכיוון שאנחנו בתחום פריקות יחידה נובע כי הם אי־פריקים.
אז f הוא מכפלה של פולינומים אי־פריקים ולכן הוא פריק מהגדרה. כעת נחשב את סכום הפולינומים המתוקנים ופריקים מדרגה 2.
מכיוון ש־$q=|\mathbb{F}|$, וראינו שיש לנו שתי צורות למבנה הפולינום המתוקן $(x-a)(x-b)$ עבור $a,b\in\mathbb{F}$ או $(x-a)^2$ עבור $a\in\mathbb{F}$.
עבור האפשרות הראשונה, יש לנו $\binom{q}{2}$ אפשרויות לבחירה ללא חזרות של $a,b\in\mathbb{F}$ ועבור המקרה השני יש לנו q אפשרויות לבחירה של $a\in\mathbb{F}$.
נסכום ונקבל שב־$\mathbb{F}[x]$ יש $q+\binom{q}{2}$ פולינומים מתוקנים מדרגה 2. $\square$

סעיף ב'

נסיק שיש $\binom{q}{2}$ פולינומים מתוקנים אי־פריקים מדרגה 2 ב־$\mathbb{F}[x]$

הוכחה: נסמן $P=\{x^2+ax+b\mid a,b\in\mathbb{F}\}$ אוסף כל הפולינומים המתוקנים ב־$\mathbb{F}[x]$.
נגדיר $\varphi:P\to\mathbb{F}_q\times\mathbb{F}_q$ על־ידי $\varphi(f(a,b))=(a,b)$ כאשר $a,b\in\mathbb{F}$ הם השורשים של f של התקנון.
נראה ש־φ היא חד־חד ערכית ועל:
על: נובע ישירות מהיות כל פולינומים ב־P מתוקן, ולכן עבור $(a,b)\in\mathbb{F}_q\times\mathbb{F}_q$ הפולינום המתוקן המתאים יהיה $x^2+ax+b=f(x)\in P$.
חד־חד ערכיות: מתקיים

$$\varphi(f(a,b))=\varphi(g(c,d))\iff(a,b)=(c,d)\iff a=c\land b=d$$

לכן φ היא חד־חד ערכית ועל ולכן $|P|=q^2$ ויש בסך־הכל q^2 פולינומים מתוקנים ב־$\mathbb{F}[x]$.
מהסעיף הקודם נסיק כי מספר הפולינום המתוקנים האי־פריקים מדרגה 2 ב־$\mathbb{F}[x]$ יהיה

$$q^2-\binom{q}{2}-q=q^2-\frac{q(q+1)}{2}=\frac{2q^2-q^2-q}{2}-\frac{q^2-q}{2}=\frac{q(q-1)}{2}=\frac{q!}{2(q-2)!}=\binom{q}{2}$$

$\square$

סעיף ג'

נמצא נוסחה למספר הפולינומים המתוקנים האי־פריקים מדרגה 3 מעל $\mathbb{F}$ ונסיק שבין רבע לשליש מהפולינומים המתוקנים מדרגה 3 הם אי־פריקים (מעל כל $\mathbb{F}$ סופי).

הוכחה: נתחיל מלהסיק מסעיף א' את המבנה האפשרי לפולינום מתוקן פריק ממעלה 3:

$$(x-a)(x-b)(x-c), (x-a)^2(x-b), (x-c)^3, (x^2+ax+b)(x-c)$$

נסכום אפשרויות בכל מקרה, משמאל לימין: במקרה הראשון יש $\binom{q}{3}$ אפשרויות.
עבור המקרה השני, נשים לב שמתקיים $(x-a)^2(x-b) \neq (x-a)(x-b)^2$ ולכן בהמשך לסעיף א' יש q^2-q אפשרויות.
למקרה השלישי יש כמובן q אפשרויות.
למקרה האחרון מסעיף א' נסיק כי יש $\frac{q(q-1)}{2}$ לפולנומים ממעלה 2, ועבור $(x-c)$ יש לנו p אפשרויות ולכן יש $\frac{q^2(q-1)}{2}$ אפשרויות.
נשים לב שזהו סכום כל הפולינומים הפריקים המתוקנים ממעלה 3:

$$\binom{q}{3}+q^2-q+q+\frac{q^2(q-1)}{2}=\frac{q!}{3!(q-3)!}+q^2+\frac{q^2(q-1)}{2}=\frac{q(q-1)(q-2)}{6}+q^2+\frac{q^3-q^2}{2}$$
$$=\frac{q^3-3q^2+2q+6q^2+3q^3-3q^2}{6}=\frac{4q^3+2q}{6}=\frac{2q^3+q}{3}$$

בדומה למה שראינו בסעיף ב', באותה דרך נוכל לבנות איזומורפיזם ולהסיק שמספר הפולינום המתוקנים ממעלה 3 הוא q^3, ולכן נקבל שמספר הפולינומים האי־פריקים מדרגה 3 יהיה:

$$q^3-\frac{2q^3+q}{3}=\frac{3q^3-2q^3-q}{6}=\frac{q^3-q}{3}$$

נרצה להסיק שבין רבע לשליש מהפולינומים המתוקנים מדרגה 3 הם אי־פריקים.
במקרה בו $q=1$ טריוויאלי.
במקרה בו $q=2$ יש בסך־הכל 8 פולינומים מתוקנים, מתוכם מהחישוב לעיל נקבל שיש 2 פולינומים אי־פריקים ממעלה 3 ($\frac{1}{4}$ מהפולינומים).
אם $q=3$ אז יש בסך־הכל 27 פולינומים מתוקנים מדרגה 3 ולפי החישוב לעיל יש 8 פולינומים מתוקנים אי־פריקים מדרגה 3 ($\sim \frac{1}{3}$ מהפולינומים).
באופן כללי, היחס בין מספר הפולינומים המתוקנים מדרגה 3 לבין מספר הפולינומים המתוקנים האי־פריקים מדרגה 3 נתון על ידי:

$$\frac{\frac{q^3}{q^3-q}}{3}=\frac{q^3}{3q(q^2-1)}=\frac{q^2}{3(q^2-1)}$$

אם נשתמש בכלים של אינפי, נחלק מונה ומכנה ב־q^2 נסיק שכאשר $q\to\infty$ המנה תשאף ל־$\frac{1}{3}$.
ראינו שהמנה לכל הפחות $\frac{1}{4}$ ושואפת ל־$\frac{1}{3}$ כאשר $q\to\infty$ ולכן קיבלנו את הנדרש. $\square$