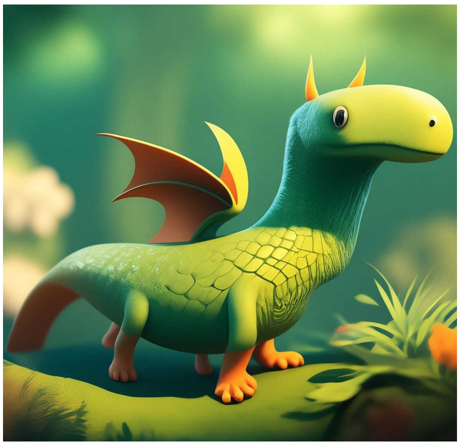
פתרון מטלה 01 — מבנים אלגבריים (2), 80446

29 במרץ 2025



שאלה 1

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

הוכחה. הגדרנו את $K[\alpha]$ כשדה הנוצר על־ידי פולינום ש־α מאפס, בפרט $K[\alpha]$ הוא שדה כך ש־$K\subseteq K[\alpha]$ עד כדי איזומורפיזם הטלה $K\to K[\alpha]$. בנוסף נבחין כי $Id:K[\alpha]\to L$ הטלת זהות היא שיכון, לכן גם $K[\alpha]\subseteq L$. מצאנו אם כן ש־$L/K[\alpha]/K$ מגדל שדות, ולכן ממשפט האינדקס מתקיים $[L:K[\alpha]]\cdot[K[\alpha]:K]=7$, לכן $[K[\alpha]:K]\in\{1,7\}$. אבל אם אינדקס זה הוא 1 אז נקבל ש־$\alpha\in K$ בסתירה להגדרתו, לכן $[K[\alpha]:K]=7$, ובהתאם נובע ש־$[L:K[\alpha]]=1$, כלומר $K[\alpha]=L$ בלבד. $\square$

שאלה 2

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

הוכחה. בהרצאה ראינו טענה שגורסת שיש תת־שדה ראשוני ב־$\mathbb{F}$, אבל כמובן $|\mathbb{Q}| > |\mathbb{F}|$ ולכן נובע ישירות שקיים ראשוני p עבורו $\mathbb{F}_p \subseteq \mathbb{F}$, ומהטענה נובע שראשוני זה הוא יחיד. נניח עתה שקיים ראשוני $q \mid |\mathbb{F}|$, אז נוכל להסיק ממשפט לגרנז' נובע שקיים איבר $\alpha \in \mathbb{F}^*$ כך ש־$\alpha^q = 1$, לכן המאפיין של השדה הוא q, אבל מאותה טענה מצאנו ש־$p = q$, ולכן רק p מחלק של $\mathbb{F}$. לבסוף נקבע $n = [\mathbb{F} : \mathbb{F}_p]$ ונקבל ש־$|\mathbb{F}| = p^n$ ישירות מהגדרת מרחבים וקטוריים סופיים. $\square$

שאלה 3

תהי L/K הרחבת שדות ותהי $S = \{s_i \mid 1 \le i \le m\} \subseteq L$.

סעיף א׳

נוכיח כי יש K־הומומורפיזם יחיד $\varphi : K[t_1, \dots, t_m] \to K[S]$ כך ש־$\varphi(t_i) = s_i$ לכל i.

הוכחה. נניח כי φ, ψ הומומורפיזמים המקיימים את הנתונים, אז $\forall i, \varphi(t_i) = \psi(t_i)$ מהגדרה. שתי ההעתקות סגורות לחיבור ולכפל, לכן אם $p_1, p_2 \in K[S]$ כך ש־$\varphi(p_j) = \psi(p_j)$ אז $\varphi(\alpha p_1 + \beta p_2) = \psi(\alpha p_1 + \beta p_2)$. לכן נותר שנבדוק הזדהות במונומים מתוקנים, כלומר איבר מהצורה $t_1^{\beta_1} \cdots t_m^{\beta_m}$,

$$\varphi(t_1^{\beta_1} \cdots t_m^{\beta_m}) = \varphi(t_1^{\beta_1}) \cdots \varphi(t_m^{\beta_m}) = \varphi(t_1)^{\beta_1} \cdots \varphi(t_m)^{\beta_m} = \psi(t_1)^{\beta_1} \cdots \psi(t_m)^{\beta_m} = \psi(t_1^{\beta_1} \cdots t_m^{\beta_m})$$

וקיבלנו כי אכן שתי ההעתקות מזדהות על כל התחום, כלומר $\varphi = \psi$. □

סעיף ב׳

נפריך את הטענה כי יש K־הומומורפיזם יחיד $\varphi : K(t_1, \dots, t_m) \to K(S)$ כך ש־$\varphi(t_i) = s_i$ לכל i.

פתרון נבחן את $\varphi : \mathbb{R}(x) \to K(\{i\}) = \mathbb{C}$ עבור $K = \mathbb{R}, L = \mathbb{C}$. נניח שקיים φ כזה, אז מתקיים $\varphi(x) = i$, ובהתאם נוכל להסיק בדומה לסעיף הקודם ש־$\varphi(f) = f(i)$ לכל פונקציה רציונלית $f \in \mathbb{R}(x)$. לבסוף נובע $\varphi(\frac{1}{x^2+1}) = \frac{1}{i^2+1} = \frac{1}{0}$, כלומר הפונקציה לא מוגדרת היטב, וזו סתירה להנחת הקיום שלה.

שאלה 4

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

סעיף א'

נוכיח שאם $\deg f = 1$ אז f ראשוני.

הוכחה. f הוא ראשוני אם ורק אם הוא אי־פריק, שכן חוג פולינומים הוא תחום אוקלידי. בהתאם נניח של־f יש פירוק כלשהו, $f = g \cdot h$ עבור $g, h \in \mathbb{F}[x]$. מטענות אודות דרגת פולינומים נסיק שמתקיים $\deg g + \deg h = \deg f$, ונובע ללא הגבלת הכלליות ש־$\deg g = 1$ וכן ש־$\deg h = 0$. אבל נקבל ש־$h = ax^0$, ו־$a \in \mathbb{F}$, לכן קיים גם a^{-1}. נגדיר מחדש את $h' = h \cdot a^{-1} = 1$ ואת $g' = g \cdot a^{-1}$ ולכן נובע $f = g' \cdot h' = g'$, כלומר f אכן אי־פריק ובהתאם ראשוני. $\square$

סעיף ב'

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

הוכחה. נניח ש־f ראשוני ויהי $\alpha \in \mathbb{F}$. אז $(x - \alpha) \nmid f$ מראשוניות, ונובע ישירות ש־$f(\alpha) \neq 0$.

בכיוון ההפוך נניח שלכל $\alpha \in \mathbb{F}$ מתקיים $f(\alpha) \neq 0$. אם $\deg f = 2$ והוא פריק נקבל בלי הגבלת הכלליות ש־$f = (x - \beta)(x - \gamma)$ עבור $\beta, \gamma \in \mathbb{F}$, ונובע ישירות ש־$f(\beta) = 0$ בסתירה, לכן נוכל להסיק ש־f אי־פריק ולכן ראשוני. נניח אם כן ש־$\deg f = 3$, ונניח שוב ש־f פריק באופן לא טריוויאלי, כלומר קיימים $f = g \cdot h$ כך ש־$\deg g = 2, \deg h = 1$, אבל אז מהנתון נובע ש־g לא מתאפס כלל וכן גם ש־h לא מתאפס, וזאת סתירה להתאפסות h כפולינום מהצורה $x - \beta$. $\square$

סעיף ג'

נראה כי הטענה מסעיף ב' לא נכונה עבור $\deg f \geq 4$.

פתרון נבחן את $f = x^4 + 1$ ב־$\mathbb{R}$. לכל $x \in \mathbb{R}$ ברור ש־$x^4 \geq 0$, ולכן גם $f(x) > 0$ ובפרט אין שורשים לפולינום זה. למרות זאת, $f = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$, כלומר f פריק.

שאלה 5

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

סעיף א׳

נוכיח ש־$\mathbb{E}$ שדה ושהוא איזומורפי לתת־השדה המינימלי של $\mathbb{R}$ שמכיל את $\sqrt[3]{5}$, כלומר $\mathbb{E} \simeq \mathbb{Q}(\sqrt[3]{5})$.

הוכחה. משאלה 4 נובע ש־x^3-5 אי־פריק מעל הרציונליים, ולכן נוכל להסיק כמסקנה מטענה מהתרגול שאכן $\mathbb{E}$ שדה.
נותר אם כן להוכיח ששני השדות איזומורפיים. נגדיר את ההומומורפיזם $\varphi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt[3]{5})$ הומומורפיזם ההצבה, ונבחין שמתקיים $\varphi(x^3-5) = 0$, כלומר $(x^3-5) \subseteq \ker\varphi$. ממשפט האיזומורפיזם הראשון נסיק שקיימים $\overline{\varphi} : \mathbb{E} \to \mathbb{Q}(\sqrt[3]{5}), \pi : \mathbb{Q}[x] \to \mathbb{E}$ כך ש־π הטלה.
מתקיים $\operatorname{Im}\overline{\varphi} = \operatorname{Im}\varphi$ וכן $\operatorname{Im}\varphi = \mathbb{Q}(\sqrt[3]{5})$, זאת שכן מבדיקה ישירה נוכל למצוא תצוגה פולינומיאלית על־ידי הצמדה ושימוש בפולינום ב־φ,
לכן מלמה מהתרגול $\overline{\varphi}$ חד־חד ערכית ועל, ונוכל להסיק ש־$\mathbb{E} \simeq \mathbb{Q}(\sqrt[3]{5})$. □

סעיף ב׳

נמצא $h \in \mathbb{Q}[x]$ המקיים $h(\sqrt[3]{5}) = \left(1 + 2\sqrt[3]{5} + 3\sqrt[3]{5}^2\right)^{-1}$.
פתרון נשתמש בשיטה שהוצגה בתרגול, נסמן $f(x) = x^3-5$ וכן $g(x) = 1+2x+3x^2$.
נבחין כי אם $q_1(x) = \frac{1}{3}x - \frac{2}{9}$ וכן $r_1(x) = \frac{1}{3}(-\frac{1}{3}x + 15 - \frac{2}{3})$ אז מתקיים $f = q_1 \cdot g + r_1$.
באופן דומה גם נגדיר $q_2(x) = 9x^2 + 9 \cdot 43x + 9 \cdot 43^2$ ו־$r_2(x) = 43^3 - 5$ ונקבל $f = q_2 \cdot (-r_1) + r_2$, וכן $\deg r_2 = 0$, לכן כמסקנה מהתרגול מתקיים,

$$h = \frac{q_1(\sqrt[3]{5}) \cdot q_2(\sqrt[3]{5})}{-r_2}$$