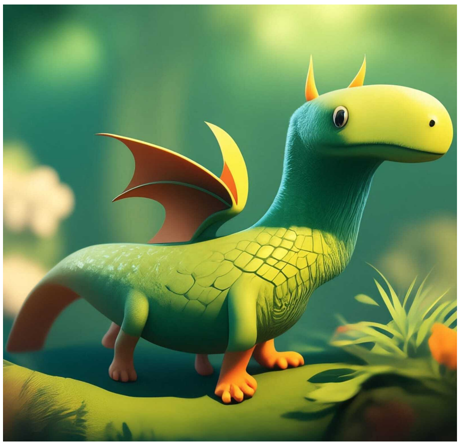
פתרון מטלה 03 — מבנים אלגבריים (2), 80446

28 באפריל 2025



שאלה 1

יהי p ראשוני ו־$n \in \mathbb{N}$, ויהי הפולינום הציקלוטומי מסדר p^n,
$$\frac{x^{p^n}-1}{x^{p^{n-1}}-1} \in \mathbb{Q}[x]$$

סעיף א׳

נראה שזהו אכן פולינום.

הוכחה. נראה ש־$x^{p^{n-1}}-1|x^{p^n}-1$. ניזכר בזהות $(1+x+\cdots+x^{n-1})(x-1) = x^n - 1$ הנכונה לכל $x \in \mathbb{C}$. לכן בפרט בהצבה $(x^{p^n})^k - 1 = (1 + x^{p^n} + \cdots + (x^{p^n})^{k-1})(x^{p^n}-1)$, נוכל להציב $k = p$ ונובע,
$$\frac{x^{p^{n+1}}-1}{x^{p^n}-1} = 1 + x^{p^n} + \cdots + (x^{p^n})^{p-1}$$
ובפרט זהו פולינום כפי שרצינו להראות. נבחין שעבור $n = 0$ הטענה נובעת ישירות מהזהות. □

סעיף ב׳

נוכיח שהפולינום הוא אי־פריק על־ידי שימוש בקריטריון אייזנשטיין.

הוכחה. כלל מקדמי הפולינום הם 1 ולכן לא נוכל להשתמש בקריטריון ישירות, נציב $x = y + 1$ ונקבל,
$$\frac{x^{p^n}-1}{x^{p^{n-1}}-1} = \frac{(y+1)^{p^n}-1}{(y+1)^{p^{n-1}}-1} = 1 + (y+1)^{p^n} + \cdots + (y+1)^{(p-1)p^n} = \sum_{i=1}^{p-1}\sum_{j=0}^{ip^n}\binom{ip^n}{j}y^j = \sum_{j=0}^{(p-1)p^n}\sum_{i=j/p^n}^{p-1}\binom{ip^n}{j}y^j$$
ולכן המקדם של y^i הוא $\sum_{i=j/p^n}^{p-1}\binom{ip^n}{j}$, כאשר בפרט $a_{(p-1)p^n} = 1$, ולכן $p \mid a_i$ לכל $i < (p-1)p^n$ אבל $p \nmid a_{(p-1)p^n}$. נבחין גם כי $a_0 = p$ ולכן $p^2 \nmid a_0$, וקריטריון אייזנשטיין חל וגורר שהפולינום הציקלוטומי מסדר p^n אי־פריק. □

שאלה 2

נפרק את $f(x)=x^4+4\in\mathbb{Q}[x]$ לפולינומים אי־פריקים מעל $\mathbb{Q}$.

פתרון נבחין כי מעל $\mathbb{C}$ ל־f, נסמן $\omega=e^{\frac{2\pi i}{4}}=e^{\frac{1}{2}\pi i}=\frac{1+i}{\sqrt{2}}$, ולכן,

$$f(x)=(x-\sqrt{2})(x-\omega\sqrt{2})(x-\omega^2\sqrt{2})(x-\omega^3\sqrt{2}i)$$

כלומר השורשים של f הם $\omega^i\sqrt{2}$ עבור $i\in\{0,1,2,3\}$. כל פולינום $g\in\mathbb{Q}[x]$ כך ש־$g\mid f$ הוא מכפלת חלק מהגורמים הלינאריים הללו, ולכן מספיק לבדוק את $2^4-1=15$ הצירופים הללו. כלל הפולינומים מסדר 1 הם מכפלות של $\sqrt{2}$ ולכן נוכל להסיק ישירות שאינם פירוק של f מעל $\mathbb{Q}$. באופן דומה לא יתכן שיהיה פולינום מחלק מדרגה 3, אחרת נקבל שאיברו החופשי הוא $2\sqrt{2}\omega_i$ עבור i כלשהו. נותר אם כן לבדוק את 6 הפולינומים מסדר 2. נוכל לפסול פולינומים שלא משלימים ל־ω בחזקה זוגית, אחרת האיבר החופשי שלהם יהיה מרוכב ובפרט לא רציונלי, ונשאר לבדוק שני פולינומים בלבד,

$$(x-\omega\sqrt{2})(x-\omega^3\sqrt{2})=x^2-\sqrt{2}(\omega+\omega^3)x+2$$

אבל מתקיים,

$$\omega+\omega^3=\frac{i+1+(-1+i)}{\sqrt{2}}=\sqrt{2}$$

ונקבל את הפולינום x^2-2x+2. מבדיקה ישירה נקבל ש־$x^4+4=(x^2-2x+2)(x^2+2x+2)$. עבור המקרה השני נקבל,

$$(x-\sqrt{2})(x-\omega^2\sqrt{2})=x^2-\sqrt{2}(1+\omega^2)x+2$$

כלומר המקדם של x הוא $\sqrt{2}(i+1)$ וזהו לא מספר רציונלי.

שאלה 3

יהיו $p_1,\dots,p_n \in \mathbb{N}$ ראשוניים שונים. נראה ש־$[\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n}) : \mathbb{Q}] = 2^n$ ושהקבוצה,
$$\mathcal{B} = \left\{ \sqrt{\prod_{i\in S} p_i} \middle| S \subseteq \{1,\dots,n\} \right\}$$
היא בסיס ל־$\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ מעל $\mathbb{Q}$.

הוכחה. אנו יודעים שמתקיים,
$$[\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] \cdots [\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n-1}})]$$
והפולינום $f_i(x) = x^2 - p_i$ מהווה פולינום מינימלי עבור כל ראשוני כזה,
$$[\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_i}) : \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{i-1}})] = 2$$
לכל i. נסיק אם כך ש־$[\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n}) : \mathbb{Q}] = 2^n$.

נוכיח את כי $\mathcal{B}$ בסיס ל־$\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ באינדוקציה על n. עבור $n = 1$ הטענה נובעת מהגדרה, כלומר $\{\sqrt{p_1}\}$ בסיס של $\mathbb{Q}(\sqrt{p_1})$. נניח כי הטענה נכונה עבור n ונבדוק את $n+1$. יהי $\alpha \in \operatorname{Sp}_{\mathbb{Q}} \mathcal{B}_n$. אילו $\alpha = 0$ אז גם $\alpha = 0 \ne p_{n+1}$, אילו $\alpha = a\sqrt{s}$ עבור $\sqrt{s} \in \mathcal{B}_n$ אז $\alpha^2 = a^2 s \in \mathbb{Q}$ ולכן לא יתכן שנגיע ל־$\sqrt{p_{n+1}}$. נניח אם כך ש־$\alpha = a_1 s_1 + \cdots + a_k s_k$, כאשר $a_i \ne 0$ לכל i. α^2 הוא חיבור של שורשי מספרים שונים ולכן לא מספר רציונלי, ונוכל להסיק שבפרט $\sqrt{p_{n+1}} \ne \alpha$. לכן נובע ש־$p_{n+1} \notin \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})$ ובהתאם $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_{n+1}}) = \mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})(\sqrt{p_{n+1}})$ וכן
$$\mathcal{B}_{n+1} = \left\{ \sqrt{\prod_{i\in S} p_i} \middle| S \subseteq \{1,\dots,n+1\} \right\}$$
$\square$

שאלה 4

בכל סעיף נגדיר את α ונחשב את $[\mathbb{Q}(\alpha):\mathbb{Q}]$.

סעיף א׳

$\alpha = \sqrt{13+6\sqrt{2}}$.

פתרון ננסה למצוא פולינום שיחסום את הערך.

$$\begin{aligned} x - \sqrt{13+6\sqrt{2}} = 0 &\iff x^2 - 13 + 6\sqrt{2} = 0 \\ &\iff x^2 - 26x + 169 - 72 = 0 \\ &\iff x^2 - 26x + 97 = 0 \end{aligned}$$

ולכן $[\mathbb{Q}(\alpha):\mathbb{Q}] \le 4$. נבחין כי $\sqrt{2} \in \mathbb{Q}(\alpha)$ ולכן $\mathbb{Q}(\alpha)/\mathbb{Q}(\sqrt{2})$, ולכן,

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})]$$

נבחן האם $\alpha \in \mathbb{Q}(\sqrt{2})$, כלומר האם קיימים $a, b \in \mathbb{Q}$ כך ש־$a + b\sqrt{2} = \alpha$,

$$a^2 + 2b^2 + 2ab\sqrt{2} = 13 + 6\sqrt{2}$$

ולכן $a^2 + 2b^2 = 13$ וכן $ab = 3$, נסיק,

$$a^2 + 2\frac{9}{a^2} - 13 = 0 \iff a^4 - 13a^2 + 18 = 0 \iff a^2 = \frac{13 \pm \sqrt{97}}{2}$$

ונסיק שלא קיימים $a, b \in \mathbb{Q}$ כאלה, ולכן $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})] \ne 1$, $2 \ge$, ולכן בהכרח,

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$$

סעיף ב׳

$\alpha = \sqrt{11+6\sqrt{2}}$.

פתרון גם הפעם $\sqrt{2} \in \mathbb{Q}(\alpha)$, ונרצה לבדוק האם $\alpha \in \mathbb{Q}(\sqrt{2})$, נקבל מתהליך דומה לסעיף הקודם כי,

$$a^2 + 2b^2 = 11 \qquad ab = 3$$

ולכן

$$a^2 + \frac{18}{a^2} - 11 = 0 \iff a^2 = \frac{11 \pm \sqrt{121 - 72}}{2} = 2, 9$$

ולכן $a = 3$ ונוכל להסיק שגם $b = 1$, כלומר $\alpha = 3 + \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ולכן,

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 1 \cdot 2$$

שאלה 5

נראה ש־$f(x) = x^2 + 4 \in \mathbb{Q}[x]$ אי־פריק, אבל ש־$f(x+a)$ לא מקיים את קריטריון אייזנשטיין לאף $a \in \mathbb{Z}$ ולאף p ראשוני.

הוכחה. נבחין כי לכל $a \in \mathbb{Z}$ מתקיים $f(x+a) = x^2 + 2ax + (a^2+4)$. נבחין גם כי $a^2 + 4 = (a+2)^2 - 2a$. על הראשוני p לחלק את $2a$, לכן $p = 2$ או $p \mid a$. אם $2 < p$ אז $p \mid 2a$ אבל $p \nmid a+2$, ולכן בהכרח $p \nmid a^2+4$, ובהכרח $p = 2$. נבחין כי $2 \nmid 1$ ולכן התנאי עבור המקדם של המעלה הגדולה ביותר כן חל, ולכן נראה ש־$p^2 = 4 \mid a^2 + 4$. אם a מספר זוגי, אז בפרט $4 \mid a^2$ וכן גם $4 \mid a^2 + 4$, ולכן תנאי הקריטריון לא חלים. נניח ש־a אי־זוגי, נובע שגם $a + 2$ אי־זוגי וכן גם $(a+2)^2$ אי־זוגי, לעומת זאת $2a$ זוגי, ולכן $a^2 + 4 = (a+2)^2 - 2a$ מספר אי־זוגי, כלומר $2 \nmid a^2 + 4$ בסתירה לדרישה ש־$p \mid a_0$. נסיק אם כך שתנאי הקריטריון לא חלים גם במקרה $p = 2$, לכן לא קיים p עבורו התנאים מתקיימים, לכל a. $\square$