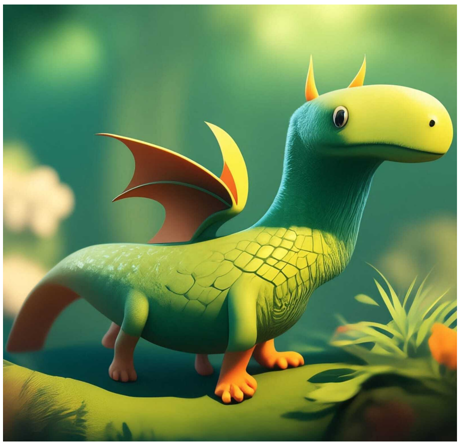
פתרון מטלה 03 — מבנים אלגבריים (2), 80446

27 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. $\square$

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. $\square$

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 $p_1, \ldots, p_n \in \mathbb{N}$ ראשוניים שונים. נראה ש־$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$ ושהקבוצה,

$$\mathcal{B} = \left\{ \sqrt{\prod_{i \in S} p_i} \middle| S \subseteq \{1, \ldots, n\} \right\}$$

היא בסיס ל־$\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ מעל $\mathbb{Q}$.

הוכחה. אנו יודעים שמתקיים,

$$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p_1}) : \mathbb{Q}] \cdots [\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})]$$

והפולינום $f_i(x) = x^2 - p_i$ מהווה פולינום מינימלי עבור כל ראשוני כזה,

$$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_i}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{i-1}})] = 2$$

לכל i. נסיק אם כך ש־$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$. $\square$