פתרון מטלה 03 — מבנים אלגבריים 2, 80446

2 במאי 2025

שאלה 1

יהי $p \in \mathbb{N}$ ראשוני ו־$n \in \mathbb{N}$. הפולינומים הציקלוטומי מסדר p^n הוא $\frac{x^{p^n}-1}{x^{p^{n-1}}-1} \in \mathbb{Q}[x]$.

סעיף א'

נראה שזה אכן פולינום, כלומר $x^{p^{n-1}}-1 \mid x^{p^n}-1$.

הוכחה: נשים לב שמתקיים

$$x^{p^n}-1 \underset{(1)}{=} x^{p \cdot p^{n-1}}-1 \underset{(1)}{=} x^{p^{(n-1)p}}-1 \underset{(2)}{=} \left(x^{p^{n-1}}-1\right) \cdot \underbrace{\left(x^{p^{(n-1)p-1}}+x^{p^{(n-1)p-2}}+...+1\right)}_{Q(x)}$$

כאשר (1) נובע מחוקי חזקות

$$p^n = p \cdot p^{n-1} \Rightarrow x^{p^n} = x^{p \cdot p^{n-1}} = x^{p^{(n-1)p}}$$

ו־(2) נובע מהזהות

$$a^p - 1 = (a-1)(a^{p-1}+a^{p-2}+...+1)$$

זאת אומרת, $x^{p^n}-1 = \left(x^{p^{n-1}}-1\right) \cdot Q(x)$ כאשר $Q(x) \in \mathbb{Q}[x]$ ולכן בפרט נובע שמתקיים

$$x^{p^{n-1}}-1 \mid x^{p^n}-1 = \left(x^{p^{n-1}}-1\right) \cdot Q(x)$$

$\square$

סעיף ב'

נוכיח שהפולינום לעיל הוא אי־פריק בעזרת קריטריון אייזנשטיין.

הוכחה: מסעיף א' אנחנו יודעים ש־$\frac{x^{p^n}-1}{x^{p^{n-1}}-1}$ זה פולינום ממעלה חיובית עם מקדמים שלמים ולכן נוכל להפעיל עליו את קריטריון אייזנשטיין.

נעשה את אותו טריק מההרצאה, נבצע החלפת משתנה $x \mapsto x+1$ ואז נקבל

$$\frac{x^{p^n}-1}{x^{p^{n-1}}-1} = \frac{(t+1)^{p^n}-1}{(t+1)^{p^{n-1}}-1} \underset{(\star)}{=} \frac{\sum_{k=1}^{p^n}\binom{p^n}{k}x^k}{\sum_{k=1}^{p^{n-1}}\binom{p^{n-1}}{k}x^k}$$

בנוגע ל־$(\star)$, נשים לב שמהבינום של ניוטון מתקיים

$$(x+1)^m = \sum_{k=0}^{m}\binom{m}{k}x^k$$

אבל לנו יש $(x+1)^m - 1$ ולכן מהפיתוח של הבינום מספיק להתחיל מאינדקס 1 בסכימה, שכן באינדקס 0 מתקיים

$$\binom{m}{0}x^0 = 1 \cdot 1 = 1$$

אזי

$$(x+1)^m - 1 = \left(\sum_{k=0}^{m}\binom{m}{k}x^k\right) - 1 = \sum_{k=1}^{m}\binom{m}{k}x^k$$

עכשיו נשים לב שלכל $1 \le k \le p^n - 1$ מתקיים מהגדרת הבינום $p \mid \binom{p^n}{k}$ ובאותו אופן לכל $1 \le t \le p^{n-1}-1$ מתקיים $p \mid \binom{p^{n-1}}{t}$, ושעבור $k = p^n$ מתקיים $\binom{p^n}{p^n} = 1$ אבל $p \nmid 1$ ועבור $t = p^{n-1}$ מתקיים באופן דומה.

ניזכר כעת בשלושת התנאים של קריטריון אייזנשטיין:

1. p לא מחלק את המקדם של המעלה הגדולה ביותר
2. p מחלק כל מקדם $0 \le i \le n-1$
3. p^2 לא מחלק את המקדם החופשי

במקרה שלנו המקדם החופשי הוא p ולכן תנאי (3) מתקיים וראינו שתנאים $(1),(2)$ מתקיימים ולכן כל תנאי קריטריון אייזנשטיין לאי־פריקות מתקיימים ולכן נקבל ש־$\frac{x^{p^n}-1}{x^{p^{n-1}}-1}$ אי־פריק ב־$\mathbb{Q}[x]$.

$\square$

שאלה 2

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

פתרון: נשים לב שעבור $f\in\mathbb{C}$ מתקיים

$$x^4+4=(x^2+2i)(x^2-2i)=(x-(1-i))\cdot(x+(1-i))\cdot(x-(1+i))x+(\dot{1}+i)$$
$$=((x-1)+i)\cdot((x+1)-i)\cdot((x-1)-i)\cdot((x+1)+i)=((x-1)^2+1)\cdot((x+1)^2+1)$$

נשים לב

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

אלו שני פולינומים ממעלה 2, ולכן לפי מטלה 2 מספיק שנשים לב שאין להם שורשים ב־$\mathbb{Q}$ (ואכן אין להם, שכן כל הפיתרונות של הפולינומים הללו הם ב־$\mathbb{C}$) ולכן אין להם שורש ב־$\mathbb{Q}$ ועל־כן הם אי־פריקים. $\square$

שאלה 3

יהיו $p_1,...,p_n \in \mathbb{N}$ ראשוניים שונים זה מזה. נראה ש־$\left[\mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_n}\right):\mathbb{Q}\right]=2^n$ ושבסיס ל־$\mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_n}\right)$ מעל $\mathbb{Q}$ נתון על־ידי

$$\mathcal{B}=\left\{\sqrt{\prod_{i\in S}p_i}\mid S\subseteq\{1,...,n\}\right\}$$

הוכחה: באינדוקציה על n, עבור $n=1$ נקבל $\left[\mathbb{Q}\left(\sqrt{p_1}\right):\mathbb{Q}\right]$, ואנחנו כבר יודעים שהפולינום המינימלי במקרה זה הוא x^2-p_1 ודרגת ההרחבה היא מדרגת הפולינום המינימלי ולכן $\left[\mathbb{Q}\left(\sqrt{p_1}\right):\mathbb{Q}\right]=2$ ובסיס במקרה זה זה הבסיס מעל $\mathbb{Q}$ שהוא 1 וגם השורש שלנו, ולכן $\mathcal{B}_1=\left\{1,\sqrt{p_1}\right\}$ מהווה בסיס (שכן, $\sqrt{p_1}\notin\mathbb{Q}$).

נניח כעת כי הטענה נכונה עבור $p_1,...,p_k$ ראשוניים שונים זה מזה ונבחר עוד $p_1,...,p_k,p_{k+1}$.

מהנחת האינדוקציה, מתקיים

$$\left[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_k}):\mathbb{Q}\right]=2^k,\mathcal{B}_k=\left\{\sqrt{\prod_{i\in S}p_i}\mid S\subseteq\{1,...,k\}\right\}$$

נניח בשלילה כי $\sqrt{p_{k+1}}\in\mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_k}\right)$, ולכן מהנחת האינדוקציה $\sqrt{p_{k+1}}$ הוא צירוף לינארי של איברי הבסיס $\mathcal{B}_k$, זאת אומרת

$$\sqrt{p_{k+1}}=\sum_{S\subseteq\{1,...,k\}}a_S\cdot\sqrt{p_S},\qquad a_S\in\mathbb{Q},p_S:=\prod_{i\in S}p_i$$

אם נעלה בריבוע, נקבל

$$p_{k+1}=\sum_{S\subseteq\{1,...,k\}}a_S^2\cdot p_S$$

משמע $p_{k+1}\in\mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_k}\right)$, אבל הנחנו שאלו ראשוניים שונים זה מזה ולכן $p_{k+1}\notin\mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_k}\right)$ וזאת סתירה.

מכפליות הדרגה מתקיים גם

$$\left[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_k},\sqrt{p_{k+1}}):\mathbb{Q}\right]=\left[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_k},\sqrt{p_{k+1}}):\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_k})\right]\cdot\left[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_k}):\mathbb{Q}\right]$$

מההוכחה לעיל נובע כי $\sqrt{p_{k+1}}\notin\mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_k}\right)$, ולכן $\left[\mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_k},\sqrt{p_{k+1}}\right):\mathbb{Q}\left(\sqrt{p_1},...,\sqrt{p_k}\right)\right]=2$ שכן הפולינום המינימלי הוא x^2-p_{k+1} ולכן

$$\left[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_k},\sqrt{p_{k+1}}):\mathbb{Q}\right]=\underbrace{\left[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_k},\sqrt{p_{k+1}}):\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_k})\right]}_{\text{2 ממה שראינו}}\cdot\underbrace{\left[\mathbb{Q}(\sqrt{p_1},...,\sqrt{p_k}):\mathbb{Q}\right]}_{2^k\text{ מהנחת האינדוקציה}}=2^{k+1}$$

עבור הבסיס, ממה שראינו נובע ישירות שניתן להוסיף את $\left\{\sqrt{p_{k+1}}\cdot b\mid b\in\mathcal{B}_k\right\}$ מהאי־תלות הלינארית ולכן

$$\mathcal{B}_{k+1}=\mathcal{B}_k\uplus\left\{\sqrt{p_{k+1}}\cdot b\mid b\in\mathcal{B}_k\right\}=\left\{\sqrt{\prod_{i\in S}p_i}\mid S\subseteq\{1,...,n\}\right\}$$

מהווה בסיס להרחבה. $\square$

שאלה 4

סעיף א'

נתון $\alpha = \sqrt{13+6\sqrt{2}}$ ונחשב את $[\mathbb{Q}(\alpha):\mathbb{Q}]$.

פתרון: נתחיל מלמצוא את $f_{\alpha/\mathbb{Q}}$, נשים לב שמתקיים

$$\alpha = \sqrt{13+6\sqrt{2}} \iff \alpha^2 = 13+6\sqrt{2} \iff (\alpha^2-13) = 6\sqrt{2} \iff \left(\alpha^2-13\right)^2 = 36\cdot 2$$
$$\iff \alpha^4 - 26\alpha^2 + 169 = 72 \iff \alpha^4 - 26\alpha^2 + 97 = 0 = f$$

המקדם המוביל הוא 1 ו־α הוא שורש שלו, נשאר לבדוק האם פולינום זה אי־פריק ב־$\mathbb{Q}$.
ניזכר שראינו במטלה 1 ובמבנים 1 שלפולינום p יש שורש α אם $p \mid (x-a)$ בחוג הפולינומים.
נניח בשלילה כי f פריק, ולכן קיים לו פירוק מהצורה

$$(x^2+ax+b)(x^2+cx+d) = x^4 + x^3(a+c) + x^2(ac+b+d) + x(ad+bc) + bd$$

במקרה שלנו צריך להתקיים

1. המקדם של x^3 הוא 0, ולכן $a+c=0 \Rightarrow c=-a$
2. המקדם של x^2 הוא -26 ולכן $ac+b+d=-26$
3. המקדם של x הוא 0 ולכן $ad+bc=0$
4. המקדם של האיבר החופשי הוא 97, ולכן $bd=97$

נציב את $c=-a$ במשוואות לעיל ונקבל את המערכת

$$ac+b+d=-26 \Rightarrow -a^2+b+d=-26$$
$$ad+bc=0 \Rightarrow ad+b(-a)=0 \Rightarrow a(d-b)=0$$

מהמשוואה השנייה נקבל שיש שני מקרים:

1. $a=0$
   במקרה זה נקבל כי $c=0$ גם־כן ומהמשוואה הראשונה נקבל $b+d=-26$, ומהמקדם החופשי נקבל $d=-26-b \Rightarrow b(-26-b) = 97 \iff b^2+26b+97=0$ נעשה נוסחת שורשים, נקבל

$$b_1,b_2 = \frac{-26\pm\sqrt{26^2+4\cdot1\cdot97}}{2\cdot1} = \frac{-26\pm\sqrt{288}}{2} = \frac{-26\pm\sqrt{144\cdot2}}{2} = \frac{-26\pm12\sqrt{2}}{2}$$

   ובעצם אין לנו פתרונות למשוואה זו ב־$\mathbb{Q}$.
2. $d=b$
   מהמשוואה הראשונה נקבל $-a^2+2b=-26 \Rightarrow b=\frac{a^2-26}{2}$, ובהצבה במקדם החופשי נקבל $bd=b^2=97 \Rightarrow b=\sqrt{97}\notin\mathbb{Q}$ ולכן שוב קיבלנו סתירה.

מצאנו שכל פירוק מוביל לשורש שלא ב־$\mathbb{Q}$ ולכן קיבלנו סתירה ו־$f(\alpha)$ הוא פולינום אי־פריק, ועל־כן עונה על כל הדרישות לפולינום מינימלי.
ראינו שדרגה של הרחבה היא כדרגת הפולינום המינימלי שלה ולכן $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$. $\square$

סעיף ב'

נתון $\alpha=\sqrt{11+6\sqrt{2}}$ ונחשב את $[\mathbb{Q}(\alpha):\mathbb{Q}]$.

פתרון: נשים לב שהפעם מתקיים

$$\alpha=\sqrt{11+6\sqrt{2}}=\sqrt{9+6\sqrt{2}+2}=\sqrt{9+6\sqrt{2}+\sqrt{2}^2}=\sqrt{\left(3+\sqrt{2}\right)^2}=3+\sqrt{2}$$

ולכן

$$(\alpha-3)^2=2\Rightarrow\alpha^2-6\alpha+9=2\iff\alpha^2-6\alpha+7=0$$

ומנוסחת שורשים מתקיים

$$\alpha_1,\alpha_2=\frac{6\pm\sqrt{36-4\cdot1\cdot7}}{2\cdot1}=\frac{6\pm\sqrt{8}}{2}$$

ואין לנו פתרונות ב־$\mathbb{Q}$, ולכן הפולינום הנ"ל אי־פריק ב־$\mathbb{Q}$, מתוקן ומתאפס בהצבת α ולכן זהו פולינום מינימלי.
ראינו שדרגה של הרחבה היא כדרגת הפולינום המינימלי שלה ולכן $[\mathbb{Q}(\alpha):\mathbb{Q}]=2$. $\square$

שאלה 5

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

הוכחה: נתחיל מלהראות ש־$f(x)$ אי־פריק מעל $\mathbb{Q}[x]$: אנחנו כבר יודעים שאין ל־$f(x)$ שורש ב־$\mathbb{Q}$ ולכן בפרט אין גורם לינארי מהצורה $x - \alpha$ כאשר α שורש ולכן מחלק את הפולינום (בפרט כל השורשים שלו מעל המרוכבים בלבד).

עבור החלק השני, נשים לב שעבור $a \in \mathbb{Z}$ מתקיים

$$f(x+a) = (x+a)^2 + 4 = x^2 + 2ax + a^2 + 4$$

אם נניח שתנאי קריטריון אייזנשטיין מתקיימים (שמותר להשתמש בהם כי זהו פולינום ממעלה חיובית עם מקדמים שלמים) , נובע שקיים $p \in \mathbb{N}$ ראשוני כך שמתקיים

1. $p \nmid 1$
2. $p \mid 2a, p \mid a^2 + 4$
3. $p^2 \nmid a^2 + 4$

מתנאי (2) נובע כי או ש־$p \mid 2$ ולכן $p = 2$ או $p \mid a$.

אם $p = 2$, אז צריך להתקיים גם $2 \mid a^2 + 4$, משמע $a^2 \equiv 0 (\operatorname{mod} 2)$ ולכן $a \in \{2k \mid k \in \mathbb{Z}\}$, ואז המקדם החופשי שלנו הוא מהצורה

$$(2k)^2 + 4 = 4k^2 + 4 = 4(k^2 + 1)$$

ואז $p^2 = 4 \mid 4(k^2 + 1)$ וזאת סתירה לתנאי (3), ולכן $p \neq 2$.

נשאר לבחון את המקרה בו $p \mid a$, ולכן $a = kp$ עבור $k \in \mathbb{Z}$, תמיד מתקיים $p \mid 2(kp)$, ונבחן את $p \mid (kp)^2 + 4$ משמע $p \mid 4$, אבל הראשוני היחידי שמחלק את 4 הוא 2 שראינו שמוביל לסתירה.

נובע אם כך כי קריטריון אייזנשטיין לא מתקיים עבור אף $a \in \mathbb{Z}$. $\square$