מבנים אלגבריים 2, 80446 — פתרון מבחן מועד א׳ 2025

31 ביולי 2025

שאלה 1

נניח כי L/K הרחבה סופית ונניח בנוסף שההרחבה פרידה (ספרבילית). אז היא פרימיטיבית (קיים $\alpha \in L$ כך ש־$L = K(\alpha)$ ו־α נקרא **איבר פרימיטיבי**).

הוכחה:

$\square$

שאלה 2

תהיי L/K הרחבת גלואה סופית ונסמן $G = \mathrm{Gal}(L/K)$.
אזי ההעתקות $\mathscr{F}(H) = L^H$, $\mathscr{G}(F) = \mathrm{Gal}(L/F)$ הפוכות אחת לשנייה ומשרות התאמה חד־חד ערכית ועל בין שדות ביניים $L/F/K$ לתתי־חבורות $1 \leq H \leq G$.

הוכחה:

$\square$

שאלה 3

בכל סעיף נקבע האם הטענה נכונה או לא נכונה וננמק לספורט.

סעיף א'

אם איברים α, β הם אלגבריים מעל שדה K אזי $\deg_K(\alpha+\beta) \le \deg_K(\alpha) + \deg_K(\beta)$.

הוכחה: הטענה **לא נכונה**.

ראינו באחד המבחנים שמתקיים $\deg_K(\alpha+\beta) \le \deg_K(\alpha) \cdot \deg_K(\beta)$ כי זה נובע מכפליות הדרגה, ובגלל שמגדל הרחבות הוא לא אדטיבי ביחס לחיבור אז לא (אין לי דוגמה נגדית). $\square$

סעיף ב'

$\sqrt{13} \in \mathbb{Q}(\xi_{13})$ כאשר ξ_{13} הוא שורש יחידה פרימיטיבי מסדר 13.

הוכחה: הטענה **נכונה**.

אפשר לעשות חישוב, ואפשר גם להיזכר מההערה שראינו במשפט אחרי סכומי גאוס: ההוכחה ההיא אומרת שגם מתקיים $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\xi_p)$.
אפשר לראות את זה מסכומי גאוס ישירות שכן $n=3 \iff 13 = p = 4n+1$ ומסכומי גאוס מתקיים $S^2 = \left(\sum_{a=1}^{12} \left(\frac{a}{12}\right)\xi_{13}^a\right)^2$ כאשר נתזכר את סימן לז'נדר

הגדרה 0.1 (סימן לז'נדר מודלו p): יהי p מספר ראשוני ($p \neq 2$) ו־$a \in \mathbb{Z}$, אז

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 (\operatorname{mod} p) \\ 1 & a \not\equiv 0 (\operatorname{mod} p) \wedge a \equiv x^2 (\operatorname{mod} p) (\text{זר ל־}p\text{ והוא שארית ריבועית מודלו }p\ a) \\ -1 & a \not\equiv 0 (\operatorname{mod} p) \wedge a \not\equiv x^2 (\operatorname{mod} p) (\text{זר ל־}p\text{ ואינו שארית ריבועית מודלו }p\ a) \end{cases}$$

במבחן ההערה מספיקה, אבל רק נבין למה זה נכון: אפשר לראות מסכומי גאוס ישירות כי $n = 3 \iff 13 = p = 4n+1$ ואז הטענה נובעת ישר, אפשר לראות גם מחישוב: בדיקה ישירה מראה שעבור $a \in \{1,3,4,9,10,12\}$ נקבל $\left(\frac{a}{13}\right) = 1$ ועבור השאר נקבל -1, אז

$$S^2 = \left(\omega - \omega^2 + \omega^3 + \omega^4 - \omega^5 - \omega^6 - \omega^7 - \omega^8 + \omega^9 + \omega^{10} - \omega^{11} + \omega^{12}\right)^2$$

אנחנו יודעים שמתקיים (מהפולינום הציקלוטומי)

$$1 + \omega + \omega^2 + \cdots + \omega^{12} = 0 \Longrightarrow \omega^1 + \omega^3 + \omega^4 + \omega^9 + \omega^{10} + \omega^{12} + 1 = -\omega^2 + \omega^5 + \omega^6 + \omega^7 + \omega^8 + \omega^{11}$$
$$\Longrightarrow S^2 = \left(2\omega^1 + 2\omega^3 + 2\omega^4 + 2\omega^9 + 2\omega^{10} + 2\omega^{12} + 1\right)^2$$

וזה חישוב רע.

אם נהיה חדי עין נשים וניזכר $\omega^k + \omega^{-k} \in \mathbb{R}$ ומתקיים $1^{-1} = 12, 3^{-1} = 10, 4^{-1} = 9$ ואז הקבוצה שלנו של $\{1,3,4,9,10,12\}$ סגורה להופכי! כלומר

$$2\omega^1 + 2\omega^{12} = 4\Re(\omega^1), \qquad 2\omega^3 + 2\omega^{10} = 4\Re(\omega^3), \qquad 2\omega^4 + 2\omega^9 = \Re(\omega^4)$$

אז נקבל ש־$S = 2\omega^1 + 2\omega^3 + 2\omega^4 + 2\omega^9 + 2\omega^{10} + 2\omega^{12} + 1 \Longrightarrow 4\Re(\omega^1 + \omega^3 + \omega^4) + 1$ ניזכר

$$\omega^k = e^{\frac{2\pi i k}{13}} = \cos\left(\frac{2\pi k}{13}\right) + i \sin\left(\frac{2\pi k}{13}\right)$$

אז

$$\Re = \omega^1 + \omega^3 + \omega^4 = \cos\left(\frac{2\pi}{13}\right) + \cos\left(\frac{6\pi}{13}\right) + \cos\left(\frac{8\pi}{13}\right)$$

ולו רק היה לנו מחשבון במבחן היינו מקבלים

$$S^2 = \left(4\left(\cos\left(\frac{2\pi}{13}\right) + \cos\left(\frac{6\pi}{13}\right) + \cos\left(\frac{8\pi}{13}\right)\right) + 1\right)^2 = 13$$

זה בדיוק אומר שמתקיים $S = \sqrt{13} = 2\omega^1 + 2\omega^3 + 2\omega^4 + 2\omega^9 + 2\omega^{10} + 2\omega^{12} + 1 \in \mathbb{Q}(\xi_{13})$. $\square$

סעיף ג'

אם K שדה ממציין חיובי, אז כל הרחבה ציקלוטומית $K(\xi_n)/K$ היא הרחבה ציקלית.

הוכחה: הטענה **נכונה**.

אנחנו כבר יודעים ש־$\mathbb{F}_p(\xi_n)/\mathbb{F}_p$ היא הרחבה ציקלוטומית וההרחבת גלואה שלה היא ציקלית.
מהגדרת הקומפוזיטום מתקיים $K(\xi_n) = \mathbb{F}_p(\xi_n)K$, ואז מתורת גלואה כל האוטומורפיזמים פועלים בצורה טריוויאלית על K ועל ξ_n, כי ברגע שעשינו את הקומפוזיטום הוספנו את כל הסקלרים שלא היו מ־K (מהגדרת הקומפוזיטום, $\mathbb{F}_p(\xi_n)K$ זה השדה הקטן ביותר שמכיל את $\mathbb{F}_p(\xi_n)$ ואת K), וזה גורר גם שהציקליות נשמרת (הרחבנו בסיס) ולכן

$$\mathrm{Gal}(K(\xi_n)/K) \simeq \mathrm{Gal}\big(\mathbb{F}_p(\xi_n)/\mathbb{F}_p\big) \simeq C_d$$

$\square$

סעיף ד'

יהי K שדה ממציין $p > 0$ ו־$f \in K[t]$ פולינום אי־פריק. אז קיים פולינום ספרבילי $g \in K[t]$ כך ש־$f(t) = g\big(t^d\big)$ עבור d מהצורה $p^n (n \in \mathbb{N})$.

הוכחה: הטענה **נכונה**.

ראינו בהרצאה אני לא יודעת באיזו טענה אבל זו טענה 14.11 בספר. $\square$

סעיף ה'

כל הרחבת שדות נורמלית מדרגה 4 מכילה תתי־הרחבה מדרגה 2.

הוכחה: הטענה **נכונה**.

אם ההרחבה ספרבילית, סיימנו. אם לא, נפרק אותה להרחבה ספרבילית והרחבה אי־ספרבילית ואז שוב נקבל שהתשובה היא כן משום מה. $\square$

שאלה 4

נמצא את כל תתי־ההרחבות הריבועיות של $\mathbb{Q}(\xi_{12})/\mathbb{Q}$ ונציגן בצורה של $\mathbb{Q}\left(\sqrt{d}\right)/\mathbb{Q}$.

פתרון: נשים לב שהפולינום האי־פריק של ההרחבה הזאת הוא $x^{12}-1$ ואנחנו יודעים שמתקיים

$$[\mathbb{Q}(\xi_{12}):\mathbb{Q}] = \varphi_{\text{אוילר}}(12) = |\{k \mid 1 \le k \le 12, \gcd(k,12)=1\}| = |\{1,5,7,11\}| = 4$$

אז בגלל שההרחבת גלואה היא מאותו סדר של ההרחבת שדות נובע כי ההרחבת גלואה שלנו היא מסדר 4 ואנחנו יודעים שמתקיים

$$\mathrm{Gal}(\mathbb{Q}(\xi_{12})/\mathbb{Q}) = (\mathbb{Z}/12\mathbb{Z})^{\times} = \{1,5,7,11\}$$

זו חבורה מסדר 4 ויש רק שתי חבורות עד־כדי איזומורפיזם שהן מסדר 4 והן חבורת קליין $V_4 \simeq C_2 \times C_2$ והחבורה הציקלית מסדר 4 שהיא C_4, אבל ההרחבה שלנו היא לא ציקלית כי

$$1 \bmod 12 = 1, 5^2 \bmod 12 = 25 \bmod 12 = 1, 7^2 = 49 \bmod 12 = 1, 11^2 = 121 \bmod 12 = 1$$

כלומר כולם מסדר 2 או 1 ואף אחד לא מסדר 4 אז לא חבורה ציקלית ולכן

$$\mathrm{Gal}(\mathbb{Q}(\xi_{12})/\mathbb{Q}) = (\mathbb{Z}/12\mathbb{Z})^{\times} \simeq V_4 \simeq C_2 \times C_2$$

עכשיו מהתאמת גלואה יש התאמה חד־חד ערכית ועל בין שדות הרחבה לבין תתי־חבורות, ואנחנו יודעים שיש לחבורת קליין בידיוק 3 תתי־חבורות לא טריוויאליות מדרגה 2 ולכן יש בידיוק 3 הרחבות שדות מדרגה 2.

נשים לב שמתקיים

$$\xi_{12} = e^{\frac{2\pi i}{12}} = e^{\frac{\pi i}{6}} = \cos\left(\frac{\pi}{6}\right) + i\sin\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} + \frac{i}{2}$$

אז $\mathbb{Q}(\xi_{12}) \subseteq \mathbb{Q}\left(i, \sqrt{3}\right)$ ונשים לב ששתי ההרחבות הללו מדרגה 4 (כי $i, \sqrt{3}$ הם בלתי־תלויים ולכן כמגדל הרחבות נקבל דרגה 4), ויש לנו הכלה בין שתי הרחבות והן מאותה דרגה אז הן אותה הרחבה.

אנחנו כבר יודעים שתתי־הרחבות ריבועיות של $\mathbb{Q}\left(i, \sqrt{3}\right)$ הן בידיוק $\mathbb{Q}\left(\sqrt{-3}\right) = \mathbb{Q}\left(i\sqrt{3}\right), \mathbb{Q}\left(\sqrt{3}\right), \mathbb{Q}\left(\sqrt{-1}\right) = \mathbb{Q}(i)$.

דרך שנייה לעשות את זה זה לפי האלגוריתם שראינו בתרגיל 8. $\square$

שאלה 5

נחשב את סכום החזקות השלישיות של הפולינום $x^3 - x + 1$.

פתרון: נסמן ב־r_1, r_2, r_3 את השורשים של הפולינום ואנחנו רוצים לחשב את $r_1^3 + r_2^3 + r_3^3$.
באופן כללי, לכל $i \in \{1,2,3\}$ מתקיים $r_i^3 = r_i - 1$, אז $r_1^3 + r_2^3 + r_3^3 = r_1 + r_2 + r_3 - 3$ ונטען שהתשובה היא -3:
נחשב

$$\begin{aligned}(x-r_1)(x-r_2)(x-r_3) &= x^3 - x^2r_3 - x^2r_1 + xr_1r_3 - x^2r_2 + xr_2r_3 + r_1r_2r_3x - r_1r_2r_3 \\ &= x^3 - x^2(r_1 + r_2 + r_3) + xr_1r_2r_3 - r_1r_2r_3\end{aligned}$$

נסמן ב־a, b, c, d את המקדמים של הפולינום שלנו $ax^3 + bx^2 + cx + d$ ובמקרה שלנו $a = 1, b = 0, c = -1, d = 1$, ולכן עם השורשים לעיל זה אמור להתאים למקדמים של הפולינום כמובן, אז

$$a = 1, b = (r_1 + r_2 + r_3) = 0, c = r_1r_2r_3 = 1, c = -r_1r_2r_3 = -1$$

ולכן

$$r_1^3 + r_2^3 + r_3^3 = r_1 + r_2 + r_3 - 3 = -3$$

□

שאלה 6

יהי f פולינום אי־פריק מעל שדה K ויהי L שדה הפיצול שלו. נניח ש־$G = \mathrm{Gal}(L/K)$ היא אבלית ונוכיח שכל שורש של f יוצר L.

הוכחה: נניח שלא ככה, ולכן עבור α שורש של f מתקיים $E = K(\alpha)$ ו־$E \subsetneq L$ ונשים לב ש־$[K(\alpha) : K] = \deg(f)$.

מהתאמת גלואה, יש התאמה חד־חד ערכית ועל בין $H \leq \mathrm{Gal}(L/K)$ לבין שדות ביניים $K \subseteq E \subseteq L$.

היות ו־G אבלית, נובע כי כל תת־חבורה שלה היא נורמלית ולכן בפרט $H = \mathrm{Gal}(L/K(\alpha)) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\alpha) = \alpha\}$ זאת־אומרת, $K(\alpha) = L^H$ ובגלל שכל תת־חבורה אבלית היא נורמלית

$$K(\sigma(\alpha)) = L^H = L^{\mathrm{Gal}(L/K(\sigma(\alpha)))} = L^{\sigma H \sigma^{-1}} = L^H = K(\alpha)$$

זה בידיוק אומר שכל השורשים של f יוצרים את אותו שדה ביניים $K(\alpha)$, אבל זה בידיוק ההגדרה של שדה פיצול ושדה פיצול יחיד עד־כדי איזומורפיזם ולכן $L \subseteq K(\alpha)$ זאת־אומרת $L = K(\alpha)$ בסתירה להנחה. $\square$

שאלה 7

נמצא את הפולינום המינימלי של $\sqrt{3}+\sqrt{5}$ מעל $\mathbb{Q}$, נראה שהוא אי־פריק מעל $\mathbb{Q}$, אי־פריק מעל $\mathbb{Z}[t]$ שנהיה פריק מודלו p לכל p ראשוני.

הוכחה: נסמן $\alpha=\sqrt{3}+\sqrt{5}$, אז

$$\alpha=\sqrt{3}+\sqrt{5}\Longleftrightarrow\alpha^2=3+2\sqrt{3}\sqrt{5}+5\Longleftrightarrow\alpha^2-8=2\sqrt{3}\sqrt{5}\Longleftrightarrow\alpha^4-16\alpha^2+64=60\Longleftrightarrow\alpha^4-16\alpha^2+4$$

נשתמש בשיטה של "Rational root theorem" ממטלה 2:

הערה (תזכורת – Rational root theorem): $f\in\mathbb{Q}[x]$ עם מקדמים שלמים ונסמן $f(x)=a_nx^n+\dots+a_1x+a_0$.
אם $\frac{r}{s}\in\mathbb{Q}$ שורש של f אז $r\mid a_0$, $s\mid a_n$

במקרה שלנו $s=1$ ו־$r=\pm1,\pm2,\pm4$, הצבה קצרה מביאה לנו שכל תוצאה לא מניבה 0 ולכן אין שורש מעל $\mathbb{Q}$ וזה אומר שאין גורם לינארי (זה בעצם אומר שאין פיצול למכפלה של $f=gh$ כאשר $\deg(g)=1,\deg(h)=3$ או ההפך).
נשאר לבחון האם יש פיצול למכפלה של $f=gh$ עם $\deg(g)=\deg(h)=2$, אז נניח בשלילה שהוא פריק, ולכן

$$\alpha^4-16\alpha^2+4=(\alpha^2+a\alpha+b)(\alpha^2+c\alpha+d)=\alpha^4+c\alpha^3+d\alpha^2+a\alpha^3+ac\alpha^2+ad\alpha+b\alpha^2+bc\alpha+bd=$$

$$\alpha^4+\alpha^3(c+a)+\alpha^2(d+ac+b)+\alpha(ad+bc)+bd$$

אז $c+a=0\Rightarrow a=-c$ וכן $bd=4$ ולכן

$$ad+bc=0\Longleftrightarrow -cd+bc=0\Longleftrightarrow bc=cd\ (2)$$

וכן

$$d+ac+b=-16\Longleftrightarrow d-c^2+b=-16$$

מ־(2) יש 2 אופציות, או ש־$c=0$ או ש־$c\neq0$.
אם $c\neq0$ אז נחלק את (2) בו ונקבל $b=d$ ולכן מכך ש־$bd=4$ אז $b=\pm2$ אבל אז למשוואה $d+ac+b=-16$ אין פיתרון כי או ש־$-4=-16$ או ש־$4=-16$ וכמובן שניהם לא נכונים.
אז $c=0$, ולכן $d+b=-16$ וגם $bd=4$, אבל גם פה נובע ש־$b=d=\pm2$ ושוב אין פיתרון ולכן ההנחה בשלילה לא נכונה והפולינום אי־פריק מעל $\mathbb{Q}$.
עכשיו, נזכר בלמה השנייה של גאוס: f פולינום אי־פריק ב־$\mathbb{Z}[\alpha]$ אם ורק אם f פרימיטיבי ואי־פריק ב־$\mathbb{Q}[\alpha]$, ונשים לב שאכן הפולינום שלנו הוא פרימטיבי כי

$$\operatorname{cont}(\alpha^4-16\alpha^2+4)=\operatorname{cont}(1,-16,4)=\gcd(1,-16,4)=1$$

ולכן הפולינום הוא פרימיטיבי ועל־כן אי־פריק מעל $\mathbb{Z}[\alpha]$ מהלמה השנייה של גאוס.
נשאר רק להראות שהוא פריק מודלו p לכל מודולו p: נסמן $y=\alpha^2$ אז $y^2-16y+7\mapsto\alpha^4-16\alpha^2+4$ ומתקיים

$$\Delta=((-16)^2-4(1))4=256-16=240$$

בבירור עבור $p=2$ הפולינום נהיה רק α^4 אז הוא פריק ונניח ש־$p\neq2$.
נזכר שיש בידיוק הרחבה ריבועית אחת $\mathbb{F}_{p^2}/\mathbb{F}_p$ ושורשים של הפולינום שלנו הם $\pm\sqrt{3},\pm\sqrt{5}$ וזה לא עוזר לי.
TODOOOOOOOOOOOOOOOOOOO? $\square$