

מבנים אלגבריים 2, 80446 — פתרון מבחן מועד ב' 2018

19 ביולי 2025



שאלה 1

נוכיח ששדה המספרים המרוכבים \mathbb{C} סגור אלגברית.

הוכחה: נזכר בשתי טענות:

1. לכל $f \in \mathbb{R}[t]$ מדרגה אי-זוגית יש שורש ב- \mathbb{R} - זה נובע ממשפט ערך הביניים: f רציפה ומתקיים $\lim_{t \rightarrow \infty} f(t) = \infty$, $\lim_{t \rightarrow -\infty} f(t) = -\infty$ ולכן בפרט יש שורש.

2. השדה \mathbb{C} סגור להוצאת שורש

כעת, נניח שלא כך ולכן יש L/\mathbb{C} הרחבה אלגברית ולכן גם L/\mathbb{R} אלגברית.

היות ו- $\text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$ נובע שכל פולינום אי-פריק הוא ספרבילי ולכן ההרחבה היא ספרבילית ולכן ניקח $L^{\text{gal}}/\mathbb{R}$ ונגדיר $G = \text{Gal}(L^{\text{gal}}/\mathbb{R})$.

ניקח $H \leq G$ תת-חבורה 2-סילו ולכן $\{e\} \leq H \leq G$ ונקבל שיש שדה ביניים $L^{\text{gal}}/F/\mathbb{R}$ כאשר $F = (L^{\text{gal}})^H$. אז $[F : \mathbb{R}] = \frac{|G|}{|H|}$ מספר אי-זוגי, זה מכיוון ש- H חבורת 2-סילו ולכן לכל $\alpha \in F$ מתקיים $\deg(f_{\alpha/\mathbb{R}})$ אי-זוגי, שכן

$$\deg(f_{\alpha/\mathbb{R}}) = [\mathbb{R}(\alpha) : \mathbb{R}] \mid [F : \mathbb{R}]$$

לכל פולינום כזה יש שורש ב- \mathbb{R} מהטענה הראשונה מתהזכורת ולכן יש ל- f_{α} שורש ב- \mathbb{R} ולכן $\alpha \in \mathbb{R}$ (אחרת, f_{α} פריק בסתירה להנחה).

אז $F = \mathbb{R}$, $H = G$ ולכן $L^{\text{gal}}/\mathbb{R}$ היא הרחבה מסדר זוגי $|G| = 2^n$ ולכן יש סדרה

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G \quad (|G_i| = 2^i)$$

מהצד השני, מהתאמת גלואה קיבלנו

$$K_n \supset \dots \supset K_2 \supset K_1 \supset \mathbb{R} \quad ([K_i : K_{i-1}] = 2)$$

נניח ש- $n \leq 2$ (בהכרח מתקיים $n \geq 1$ כי $\mathbb{C} \subset L^{\text{gal}}$), אבל זו סתירה כי אז נקבל

$$\mathbb{R} \neq K_1 = \mathbb{R}(\sqrt{a})$$

אבל $a \in \mathbb{R}$ ולכן בהכרח $a < 0$ ואז $K_1 = \mathbb{C}$, אבל $K_2 = \mathbb{C}(\sqrt{a+bi}) \neq K_1 = \mathbb{C}$ אבל אז סתירה לטענה השנייה מהתזכורת, ולכן בהכרח $n = 1$ \square

$L = \mathbb{C}$ בסתירה לכך ש- L לא טריוויאלית, כנדרש.

שאלה 2

נוכיח שכל פולינום פרימיטיבי $f(x) \in \mathbb{Z}[x]$ שהוא אי-פריק ב- $\mathbb{Z}[x]$ הוא גם אי-פריק ב- $\mathbb{Q}[x]$.

הוכחה: נזכר בשתי הגדרות

הגדרה 0.1 (תכולה): עבור פולינום $f(t) \in \mathbb{Z}[t]$ (תזכורת: $f(t) = \sum_{i=0}^n a_i t^i$) נגדיר תכולה של f להיות

$$\text{cont}(f) = \gcd(a_0, a_1, \dots, a_n)$$

הגדרה 0.2 (פולינום פרימיטיבי): פולינום $f(t) \in \mathbb{Z}[t]$ יקרא פרימיטיבי אם $\text{cont}(f) = 1$.

הערה: לכל פולינום f יש פירוק ב- $\mathbb{Z}[t]$ הנתון על-ידי $f = \text{cont}(f) \cdot f_0(t)$ כאשר $f_0(t)$ הוא פולינום פרימיטיבי.

וניזכר בלמת גאוס הראשונה:

משפט 0.1 (למת גאוס הראשונה): אם $f, g \in \mathbb{Z}[t]$ אזי $\text{cont}(fg) = \text{cont}(f) \cdot \text{cont}(g)$. בפרט, fg פרימיטיבי אם ורק אם f ו- g פרימיטיביים.

הוכחה: מההערה לעיל מתקיים $f \cdot g = \text{cont}(f) \cdot \text{cont}(g) \cdot \underbrace{f_0 \cdot g_0}_{\text{פרימיטיביים}}$ ולכן מספיק להוכיח כי $f_0 \cdot g_0$ הוא פרימיטיבי:

נניח שלא ולכן קיים $p \in \mathbb{N}$ ראשוני כך שמתקיים $p \mid \text{cont}(f_0 \cdot g_0)$. אבל $f_0 = \sum_{i=0}^n a_i t^i, g_0 = \sum_{j=0}^m b_j t^j$ הם פולינומים פרימיטיביים (ולכן לא כל a_i, b_j מתחלקים ב- p) ולכן נוכל לבחור m, n מינימליים כך ש- $p \nmid a_n$ ו- $p \nmid b_m$. נסתכל על המקדם של $c = \sum_{k=0}^{m+n} a_k b_{m+n-k} t^{m+n}$ ב- $f_0 \cdot g_0$, נכתוב אותו מפרשות:

$$\underbrace{a_0 b_{m+n} + \dots + a_{n-1} b_{m+1}}_{\text{מתחלקים ב-} p \text{ לכל } k < n} + a_n b_m + \underbrace{a_{n+1} b_{m-1} + \dots + a_{m+n} b_0}_{\text{מתחלקים ב-} p \text{ כי } p \mid b_k \text{ לכל } k > n}$$

אבל $a_n b_m$ זר לחלוקה ב- p ולכן $c \nmid p$ וזאת סתירה.

נוכיח למה שהייתה חלק מלמת גאוס השנייה:

למה 0.1: יהי $f \in \mathbb{Z}[t]$ פולינום לא קבוע. נזכור כי $\mathbb{Q}[t]$ הוא $\text{Frac}(\mathbb{Z})$, שדה השברים של $\mathbb{Z}[t]$.

אם $f = g \cdot h$ פירוק ב- $\mathbb{Q}[t]$ אזי קיים $c \in \mathbb{Q}^\times, c \neq 0$ כך ש- $c \cdot g, c^{-1} \cdot h \in \mathbb{Z}[t]$ ולכן $f = (c \cdot g) \cdot (c^{-1} \cdot h)$ פירוק ב- $\mathbb{Z}[t]$.

הוכחה: ניקח את הפירוק $f = g \cdot h$ עבור $g, h \in \mathbb{Q}[t]$ וניקח $0 < m, n \in \mathbb{Z}$ ונזכור $m \cdot g, n \cdot h \in \mathbb{Z}[t]$ ואז נקבל פירוק $m \cdot n \cdot f = m \cdot g \cdot n \cdot h$ נסמן $\ell = \text{cont}(f), \alpha = \text{cont}(m \cdot g), \beta = \text{cont}(n \cdot h)$ מלמת גאוס הראשונה נקבל עם כפליות התכולה

$$\text{cont}(m \cdot n \cdot f) = m \cdot n \cdot \ell = \alpha \cdot \beta = \text{cont}(m \cdot g \cdot n \cdot h)$$

אם כך, ניקח $m \cdot n \cdot f = m \cdot g \cdot n \cdot h$ ונחלק ב- $\alpha \beta$ נקבל $\frac{m \cdot n \cdot f}{\alpha \beta} = \frac{m}{\alpha} \cdot g \cdot \frac{n}{\beta} \cdot h$ משמע $\frac{1}{\ell} \cdot f = \frac{m \cdot n \cdot f}{m \cdot n \cdot \ell} = \underbrace{\frac{m}{\alpha} \cdot g \cdot \frac{n}{\beta} \cdot h}_{\in \mathbb{Z}[t]}$.

נשאר רק להוכיח את הטענה שלנו: נניח כי f אי-פריק ב- $\mathbb{Z}[t]$ ולכן $f = \text{cont}(f) \cdot \frac{f}{\text{cont}(f)}$ פירוק טריוויאלי ונשים לב $\deg\left(\frac{f}{\text{cont}(f)}\right) > 0$ ולכן $\text{cont}(f)$ הפך ולכן f פרימיטיבי.

נניח ש- f פריק ב- $\mathbb{Q}[t]$ ולכן יש $f = g \cdot h$ כך ש- $\deg(g), \deg(h) > 0$ ולכן מהלמה לעיל נקבל $f = c \cdot g \cdot c^{-1} \cdot h$ עם דרגות גדולות מ-0 ב- $\mathbb{Z}[t]$ משמע הוא פריק בו, וזאת סתירה.

שאלה 3

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

סעיף א'

אם K שדה ממציין $p > 0$ כך ש- $K^p = K$ אז ההעתקה $f: K \rightarrow K$ הנתונה על-ידי $x^{\frac{1}{p}}$ היא אוטומורפיזם של K .
הוכחה: הטענה נכונה.

כדי להראות אוטומורפיזם עלינו להראות שזה הומומורפיזם, חד-חד ערכי ועל:

1. זה הומומורפיזם

1. ניזכר שמהבינום כמו תמיד נקבל $f(x+y) = (x+y)^p = x^p + y^p = f(x) + f(y)$ אבל בגלל שהשדה פרפקטי מתקיים

$$(x+y)^{\frac{1}{p}} = (x^p + y^p)^{\frac{1}{p}} \iff (x+y)^{\frac{1}{p}} = \left(x^{\frac{1}{p}} + y^{\frac{1}{p}}\right)^p$$

$$f(x+y) = f(x) + f(y) \text{ ולכן}$$

$$f(xy) = (xy)^{\frac{1}{p}} = x^{\frac{1}{p}}y^{\frac{1}{p}} = f(x)f(y) \quad 2.$$

2. חד-חד ערכי כי מההנחה על היות השדה מושלם, לכל איבר יש שורש מסדר p ייחודי כי

$$f(x) = f(y) \iff x^{\frac{1}{p}} = y^{\frac{1}{p}} \iff \left(x^{\frac{1}{p}}\right)^p = \left(y^{\frac{1}{p}}\right)^p \iff x = y$$

3. על כי אם ניקח $z \in K$ ונבחר $x = z^p$ אז $f(x) = (z^p)^{\frac{1}{p}} = z$

אז זה אוטומורפיזם (הוא כמובן משמר גם את שדה הבסיס כי לכל $a \in \mathbb{F}_p$ מתקיים $f(a) = a^{\frac{1}{p}} = a$).

□

סעיף ב'

יהיו K, L, F שדות כך ש- $K \subseteq L \subseteq \bar{K}$ ו- $K \subseteq F \subseteq \bar{K}$.

אם $L/K, F/K$ הן הרחבות גלואה סופיות אז גם $(FL)/K$ היא גלואה סופית ו- $\text{Gal}((FL)/K)$ היא תת-חבורה של $\text{Gal}(F/K) \times \text{Gal}(L/K)$.

הוכחה: הטענה נכונה.

ראינו אותה בהרצאה אבל אין לי מושג על מה מדובר.

□

סעיף ג'

לשדה $\mathbb{F}_p(t)$ יש הרחבה לא פרידה עם מעלת הרחבה p .

הוכחה: הטענה נכונה.

ניקח $f(x) = x^p - a$ עם $a \in \mathbb{F}_p$, זה פולינום מדרגה p ובשדה \mathbb{F}_p אין לו p שורשים שונים (כי $f'(x) = px^{p-1} \equiv 0 \pmod{p}$ וזה אומר שכל השורשים שלו כפולים, זאת-אומרת הפולינום אי-פריד).

אנחנו רוצים שבשדה הרחבה השורשים של הפולינום שלנו יהיו $\alpha = a^{\frac{1}{p}}$, אז ניקח את ההרחבה $\mathbb{F}_p(\alpha)$ והפולינום שלנו זה הפולינום המינימלי שלה ולכן ההרחבה היא מדרגה p .

□

סעיף ד'

כל הרחבות שדות סופית K/\mathbb{Q} היא גלואה.

הוכחה: הטענה לא נכונה.

ניקח $K = \mathbb{Q}(\sqrt[3]{2})$ זו הרחבה מדרגה 3 שאיננה נורמלית (ולכן בהכרח אינה גלואה) כי $\sqrt[3]{2}\xi_3 \notin \mathbb{Q}(\sqrt[3]{2})$ למרות שהשורש הזה צמוד ל- $\sqrt[3]{2}$ ולכן ההרחבה לא מכילה את הפיצול של הפולינום ולכן לא נורמלית.

□

שאלה 4

נבנה הרחבות נורמליות $F/K, L/F$ כך שהרחבה L/K לא נורמלית.

הוכחה: נבחר $K = \mathbb{Q}, F = \mathbb{Q}(\sqrt{2}), L = \mathbb{Q}(\sqrt[4]{2})$.

אנחנו כבר יודעים ש- $F/K = \mathbb{Q}(\sqrt{2})/\mathbb{Q}$ היא נורמלית (הרחבה ריבועית היא נורמלית) וגם $L/K = \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ היא איננה נורמלית כי הפולינום המינימלי של ההרחבה הוא $x^4 - 2$ ולא כל השורשים נמצאים בהרחבה $(i\sqrt[4]{2}, -i\sqrt[4]{2})$.

נטען כעת שהרחבה $L/F = \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ היא נורמלית.

נסתכל על הפולינום $x^2 - \sqrt{2}$ הוא אי-פריק מעל $\mathbb{Q}(\sqrt{2})$ ושורשיו הם $\pm\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$ וזו בדיקת ההגדרה לנורמליות (כי הוא מתפצל לחלוטין עכשיו ב- L), ולכן L/F הרחבה נורמלית.

□

שאלה 5

נמצא את חבורת הגלואה של הרחבת השדות $F_{11}(\xi_7)/F_{11}$ כאשר ξ_7 הוא שורש יחידה פרימיטיבי מסדר 7. הוכחה: קודם כל

$$F_{11}^\times = \{1, \dots, 10\} \cong C_{10}$$

אז אנחנו רוצים את החזקה המינימלית שבה נמצא את כל שורשי היחידה מסדר 7, וזה יקרה מתי שיתקיים $11^k - 1 \mid 7$, עכשיו $11 \bmod 7 = 4$ אז אנחנו צריכים למצוא חזקה של 4 שבמודול 7 מביאה לנו 1 (כי אנחנו רוצים $\langle \xi_7 \in \langle \xi_{11^n-1} \rangle$)

$$\underbrace{4^1 = 4 \bmod 7}_x, \underbrace{4^2 = 16 \bmod 7 = 2}_x, \underbrace{4^3 = 64 \bmod 7 = 1}_\checkmark$$

ולכן $F_{11}(\xi_7) = \mathbb{F}_{11^3}$ כי עבור חזקת 3 זו החזקה המינימלית מעל השדה שבו $x^7 - 1$ מתפצל לחלוטין ומתקיים $[\mathbb{F}_{11^3} : \mathbb{F}_{11}] = 3$. ראינו שהשדה \mathbb{F}_{p^n} הוא הרחבת גלואה של \mathbb{F}_p ושכל הרחבה סופית של שדה סופי היא גלואה וראינו ש- $G = \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ היא חבורה ציקלית הנוצרת על ידי אוטומורפיזם פרובניוס $\text{Fr}(x) = x^p$ (בסיכומי הרצאות של מיכאל טענה 6.2.6, וזו הרחבת גלואה באמצעות מסקנה 17.4 בספר – \mathbb{F}_{p^n} הוא הרחבת גלואה של \mathbb{F}_p מהיותו שדה פיצול של פולינום $x^{p^n} - x$ מעל כל שדה ביניים $\mathbb{F}_p \subseteq M \subseteq \mathbb{F}_{p^n}$ ולכן הוא גם גלואה מעל M וזה שדה פרפקטי) במקרה שלנו מתקיים $3 = [\mathbb{F}_{p^3} : \mathbb{F}_p] = |G|$ ולכן $G \cong \mathbb{Z}/3\mathbb{Z}$ עבור $\text{Fr}(x) = x^{11}$.

□

שאלה 6

$\sqrt{2}, \sqrt[3]{3}$ השורשים הממשיים החיוביים, נוכיח שההרחבה $\mathbb{Q}(\sqrt{2} + \sqrt[3]{3})/\mathbb{Q}$ איננה נורמלית.

הוכחה: נסמן

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ אלגברי מעל } \mathbb{Q}\}$$

ניזכר ש- $\overline{\mathbb{Q}}$ הוא שדה סגור אלגברית ו- $\overline{\mathbb{Q}}/\mathbb{Q}$ הרחבת שדות אלגברית, אז

$$\text{Aut}(\overline{\mathbb{Q}}/\mathbb{Q}) = \{\sigma \in \text{Aut}(\overline{\mathbb{Q}}) \mid \forall x \in \mathbb{Q}, \sigma(x) = x\}$$

ואנחנו יודעים ש- $\sqrt{2}, \sqrt[3]{3} \in \overline{\mathbb{Q}}$ עבור הפולינומים $x^2 - 2, x^3 - 3$ וכמובן $\sqrt{2}, \sqrt[3]{3} \notin \mathbb{Q}$ ולכן יש $\sigma \in \text{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ כך שמתקיים

$$\sigma(\sqrt{2}) = \pm\sqrt{2}, \sigma(\sqrt[3]{3}) = \sqrt[3]{3}\xi_3$$

אז בפרט $\sigma(\mathbb{Q}(\sqrt{2} + \sqrt[3]{3})) \ni \pm\sqrt{2} + \sqrt[3]{3}\xi_3$ זאת אומרת בהכרח יש לנו צמוד של $\sqrt{2} + \sqrt[3]{3}$ שלא נמצא בהרחבה ועל-כן בפרט ההרחבה איננה נורמלית.

□

שאלה 7

נמצא α אלגברי מעל \mathbb{Q} כך ש- $\mathbb{Q}(\alpha)/\mathbb{Q}$ היא הרחבת גלואה ו- $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \mathbb{Z}/5\mathbb{Z}$.
הוכחה: הכי קל לקחת הרחבה ציקלוטומית ונוסיף שורש יחידה מסדר כלשהו שיתן לנו הרחבה בגודל המתאים אז $\alpha = \xi_n$ כלשהו (זה יהיה אלגברי כי זה שורש של הפולינום $x^n - 1$).
ניזכר ש-

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi_{\text{אייילר}}(n) = |\{k \mid 1 \leq k \leq n, \gcd(k, n) = 1\}|$$

המועד הראשון הוא $n = 5$ אבל $|\mathbb{Z}/5\mathbb{Z}| = 5 \neq 4 = |\{1, 2, 3, 4\}| = \varphi_{\text{אייילר}}(5)$.
נעבוד באלימות כי אין לי רעיון אחר:

$$\varphi_{\text{אייילר}}(6) = |\{1, 5\}| = 2 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$$

$$\varphi_{\text{אייילר}}(7) = |\{1, 2, 3, 4, 5, 6, 7\}| = 7 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$$

$$\varphi_{\text{אייילר}}(8) = |\{1, 3, 5, 7\}| = 4 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$$

$$\varphi_{\text{אייילר}}(9) = |\{1, 2, 4, 5, 7, 8\}| = 6 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$$

$$\varphi_{\text{אייילר}}(10) = |\{1, 3, 7, 9\}| = 4 \neq 5 = |\mathbb{Z}/5\mathbb{Z}| \quad \varphi_{\text{אייילר}}(11) = |\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}| = 10 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$$

אז אולי לא.

אנחנו רוצים למצוא הרחבת גלואה עם חבורת גלואה $\mathbb{Z}/5\mathbb{Z}$, אז אנחנו שואלים עבור איזה n נקבל ש- $(\mathbb{Z}/n\mathbb{Z})^\times$ הוא חבורה ציקלית עם סדר שמתחלק ב-5 כדי שתהיה תת-חבורה ציקלית מסדר 5.

ובידויק מהרשימה שלנו למעלה זה קורה כאשר מסתכלים על ההרחבה $[\mathbb{Q}(\xi_{11}) : \mathbb{Q}] = 10$ ואז $\text{Gal}(\mathbb{Q}(\xi_{11})/\mathbb{Q}) \cong \mathbb{Z}_{10}$, ואנחנו יודעים ממשפט השאריות הסיני

$$\mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_5$$

אנחנו צריכים עכשיו להשתמש בהתאמת גלואה כדי לקבל את היחסים הפוכים בין תתי-חבורות לבין תתי-שדות בהרחבה.
כמובן שכל $\sigma \in G$ מזיזה רק את ξ_{11} אז אם נסתכל על

$$H = \langle \xi_{11} \mapsto \xi_{11}^2 \rangle = \{ \xi_{11} \mapsto \xi_{11}^{2^n} \mid 1 \leq n \leq 5 \}$$

□

היא כמובן מסדר 5 שכן (למה? כובע) אז אם נבחר $\alpha = \xi_{11} + \overline{\xi_{11}}$ מסיים.