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

18 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 $\lim\limits_{t \to \infty} f(t) = \infty, \lim\limits_{t \to -\infty} f(t) = -\infty$ 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־$\operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = 0$ נובע שכל פולינום אי־פריק הוא ספרבילי ולכן ההרחבה היא ספרבילית ולכן ניקח $L^{\text{gal}}/\mathbb{R}$ ונגדיר $G = \operatorname{Gal}\left(L^{\text{gal}}/\mathbb{R}\right)$.
ניקח $H \le G$ תת־חבורה 2־סילו ולכן $\{e\} \le H \le G$ ונקבל שיש שדה ביניים $L^{\text{gal}}/F/\mathbb{R}$ כאשר $F = \left(L^{\text{gal}}\right)^H$.
אז $[F : \mathbb{R}] = \frac{|G|}{|H|}$ מספר אי־זוגי, זה מכיוון ש־H חבורת 2־סילו ולכן לכל $\alpha \in F$ מתקיים $\deg\left(f_{\alpha/\mathbb{R}}\right)$ אי־זוגי, שכן

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

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

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G \qquad \left(|G_i| = 2^i\right)$$

מהצד השני, מהתאמת גלואה קיבלנו

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

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

$$\mathbb{R} \ne K_1 = \mathbb{R}\left(\sqrt{a}\right)$$

אבל $a \in \mathbb{R}$ ולכן בהכרח $a < 0$ ואז $K_1 = \mathbb{C}$, אבל $C \ne K_2 = \mathbb{C}\left(\sqrt{a + bi}\right)$ אבל זו סתירה לטענה השנייה מהתזכורת, ולכן בהכרח $n = 1 \Rightarrow$ $L = \mathbb{C}$ בסתירה לכך ש־L לא טריוויאלית, כנדרש. $\square$

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: $f(t)=\sum_{i=0}^{n}a_it^i$) נגדיר **תכולה** של f להיות

$$\mathrm{cont}(f)=\gcd(a_0,a_1,...,a_n)$$

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

הערה: לכל פולינום f יש פירוק ב־$\mathbb{Z}[t]$ הנתון על־ידי $f=\mathrm{cont}(f)\cdot f_0(t)$ 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 $\mathrm{cont}(fg)=\mathrm{cont}(f)\cdot\mathrm{cont}(g)$. בפרט, fg פרימיטיבי אם ורק אם f ו־g פרימיטיביים.

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

נניח שלא ולכן קיים $p\in\mathbb{N}$ ראשוני כך שמתקיים $p\mid\mathrm{cont}(f_0\cdot g_0)$, אבל $f_0=\sum_{i=0}^{n}a_it^i,g_0=\sum_{j=0}^{m}b_jt^j$ 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 t^{m+n} של $c=\sum_{k=0}^{m+n}a_kb_{m+n-k}$ ב־$f_0\cdot g_0$, נכתוב אותו מפרושות:

$$\underbrace{a_0b_{m+n}+...+a_{n-1}b_{m+1}}_{\text{מתחלקים ב־p כי } p|a_k \text{ לכל k<n}}+a_nb_m+\underbrace{a_{n+1}b_{m-1}+...+a_{m+n}+b_0}_{\text{מתחלקים ב־p כי } p|b_k \text{ לכל k>n}}$$

אבל a_nb_m זר לחלוקה ב־p ולכן $p\nmid c$ וזאת סתירה. $\square$

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 $\mathrm{Frac}(\mathbb{Z})$, שדה השברים של $\mathbb{Z}[t]$.

אם $f=g\cdot h$ פירוק ב־$\mathbb{Q}[t]$ אזי קיים $0\neq c\in\mathbb{Q}^\times$ 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 $0<m,n\in\mathbb{Z}$ כך ש־$m\cdot g,n\cdot h\in\mathbb{Z}[t]$ ואז נקבל פירוק $m\cdot n\cdot f=m\cdot g\cdot n\cdot h$. נסמן $\ell=\mathrm{cont}(f),\alpha=\mathrm{cont}(m\cdot g),\beta=\mathrm{cont}(n\cdot h)$. מלמת גאוס הראשונה נקבל עם כפליות התכולה

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

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

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

$\square$

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 $f : K \to K$ 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 $f(x+y) = (x+y)^p = x^p + y^p$ אבל בגלל שהשדה פרפקטי מתקיים
   $$(x+y)^{\frac{1}{p}} = (x^p + y^p)^{\frac{1}{p}} \iff (x+y)^{\frac{1}{p}} = \left(x^{\frac{1}{p}} + y^{\frac{1}{p}}\right)$$
   ולכן $f(x+y) = f(x) + f(y)$
   2. $f(xy) = (xy)^{\frac{1}{p}} = x^{\frac{1}{p}} y^{\frac{1}{p}} = f(x)f(y)$
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־$K \subseteq L \subseteq \overline{K}$ ו־$K \subseteq F \subseteq \overline{K}$.

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

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 $f'(x) = px^{p-1} \underset{\mathrm{mod}\, p}{\equiv} 0$ 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 $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ זו הרחבה מדרגה 3 שאיננה נורמלית (ולכן בהכרח אינה גלואה) כי $\sqrt[3]{2}\xi_3 \notin \mathbb{Q}\left(\sqrt[3]{2}\right)$ 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 שההרחבה L/K לא נורמלית.

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

אנחנו כבר יודעים ש־$F/K=\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ היא נורמלית (הרחבה ריבועית היא נורמלית) וגם $L/K=\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ 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 שההרחבה $L/F=\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$ היא נורמלית.

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

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

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

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

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

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־$G = \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}\right)$ היא חבורה ציקלית הנוצרת על־ידי אוטומורפיזם פרובניוס $\mathrm{Fr}(x) = x^p$ (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 $|G| = \left[\mathbb{F}_{p^3} : \mathbb{F}_p\right] = 3$ ולכן $G \cong \mathbb{Z}/3\mathbb{Z}$ עבור $\mathrm{Fr}(x) = x^{11}$.

$\square$

שאלה 6

$\sqrt{2},\sqrt[3]{3}$ השורשים הממשיים החיובים, נוכיח שההרחבה $\mathbb{Q}\left(\sqrt{2}+\sqrt[3]{3}\right)/\mathbb{Q}$ 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

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

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 $\sigma\in\mathrm{Aut}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ כך שמתקיים

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

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

שאלה 7

נמצא α אלגברי מעל $\mathbb{Q}$ כך ש־$\mathbb{Q}(\alpha)/\mathbb{Q}$ היא הרחבת גלואה ו־$\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \mathbb{Z}/5\mathbb{Z}$.

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־

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

המועד הראשון הוא $n = 5$ אבל $\varphi_{\text{אוילר}}(5) = |\{1,2,3,4\}| = 4 \neq 5 = |\mathbb{Z}/5\mathbb{Z}|$.

נעבוד באלימות כי אין לי רעיון אחר:

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

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.

ובידיוק מהרשימה שלנו למעלה זה קורה כאשר מסתכלים על ההרחבה $[\mathbb{Q}(\xi_{11}) : \mathbb{Q}] = 10$ ואז $\mathrm{Gal}(\mathbb{Q}(\xi_{11})/\mathbb{Q}) \cong \mathbb{Z}_{10}$, 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 ההפוכים בין תתי־חבורות לבין תתי־שדות בהרחבה.

כמובן שכל $\sigma \in G$ מזיזה רק את ξ_{11} אז אם נסתכל על

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

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