מבנים אלגבריים 2, 80446 — פתרון מבחן מועד ב' 2021

23 ביולי 2025

שאלה 1

השדה $\mathbb{C}$ 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 $\lim_{t\to\infty} f(t) = \infty, \lim_{t\to-\infty} f(t) = -\infty$ 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־$\mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$ נובע שכל פולינום אי־פריק הוא ספרבילי ולכן ההרחבה היא ספרבילית ולכן ניקח $L^{\mathrm{gal}}/\mathbb{R}$ ונגדיר $G = \mathrm{Gal}\left(L^{\mathrm{gal}}/\mathbb{R}\right)$.
ניקח $H \leq G$ תת־חבורה 2־סילו ולכן $\{e\} \leq H \leq G$ ונקבל שיש שדה ביניים $L^{\mathrm{gal}}/F/\mathbb{R}$ כאשר $F = \left(L^{\mathrm{gal}}\right)^H$.
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 $L^{\mathrm{gal}}/\mathbb{R}$ היא הרחבה מסדר זוגי $|G| = 2^n$ ולכן יש סדרה

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

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

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

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

שאלה 2

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

הוכחה: נוכיח כי לכל שדה ביניים $L/F/K$ מתקיים $F=L^{\mathrm{Gal}(L/F)}$.
ברור כי $F\subseteq L^{\mathrm{Gal}(L/F)}$ כי $\mathrm{gal}(L/F)$ אלו האוטומורפיזמים שמקבעים את F.
ניקח $\alpha\in L/F$ ולכן α פריד מעל F כי L/K פרידה (כי גלואה) ולכן L/F פרידה ו־$\deg_s(\alpha)>1$ ולכן יש לו צמוד α' מעל F ולכן קיים $\sigma\in\mathrm{Aut}_F\big(\overline{F}\big)$ כך שיתקיים $\sigma(\alpha)=\alpha'$.
מתקיים $\sigma|_K=\mathrm{Id}_K$ וגם $\sigma(L)=L$ מהיות L/K נורמלית ולכן $\sigma|_L\in\mathrm{Gal}(L/F)$ כי הוא הזהות על F, אבל $\sigma(\alpha)\neq\alpha$ ולכן $\alpha\in L^{\mathrm{Gal}(L/F)}$ ולכן קיבלנו שיוויון ומתקיים $F=L^{\mathrm{Gal}(L/F)}$.
אז מתקיים

$$\mathscr{F}(\mathscr{G}(F))=\mathscr{F}(\mathrm{Gal}(L/F))=L^{\mathrm{Gal}(L/F)}=F\Rightarrow\mathscr{F}\circ\mathscr{G}=\mathrm{Id}$$

בכיוון השני, נזכר במשפט ארטין:

משפט 0.1 (משפט ארטין): L שדה ו־$H\le\mathrm{Aut}(L)$ חבורת אוטומורפיזמים סופית כלשהי ונסמן $F=L^H$. אז L/F הרחבת גלואה ו־$H=\mathrm{Gal}(L/F)$.

בכיוון השני, ניקח $H\le G$ תת־חבורה ולכן ממשפט ארטין (יחד עם הסופיות!) נקבל

$$H=\mathrm{Gal}\big(L/L^H\big)=\mathscr{G}(\mathscr{F}(H))\Rightarrow\mathscr{G}\circ\mathscr{F}=\mathrm{Id}$$

אז הוכחנו את ההתאמתה ונשאר להראות ש־$\mathscr{G},\mathscr{F}$ הופכות שיכונים:
נניח כי $H'\le H\le G$ תתי־חבורות של G אז $\mathscr{F}(H)=L^H$ אלו כל האיברים ב־L שנשארים במקום על־ידי פעולת H, אבל $H'\subseteq H$ ולכן נובע כי אם איבר נשאר במקום על־ידי H הוא ישאר במקום גם על־ידי H' ולכן $\mathscr{F}(H)\subseteq L^{H'}=\mathscr{F}(H')$.
ניקח שדות ביניים $L/F/F'/K$ אז $\mathscr{G}(F)=\mathrm{Gal}(L/F)$ אלו אוטומורפיזמים המשמרים את F אבל $F'\subseteq F$ ולכן הם גם משמרים הכרח את F', כלומר $\mathscr{F}=\mathrm{Gal}(L/K)\subseteq\mathrm{Gal}(L/F')=\mathscr{G}(F')$, כנדרש. $\square$

שאלה 3

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

סעיף א'

כל אוטומורפיזם של שדה סופי הוא חזקה של פרובניוס.

הוכחה: הטענה **נכונה**.

זאת מכיוון שהפרובניוס יוצר את חבורת האוטומורפיזמים (כי $\mathbb{F}_p^\times$ היא חבורה ציקלית ולכן היא נוצרת על־ידי איבר אחד, g, ואנחנו צריכים להעלות את g לחזקה של p כדי לקבל שוב את g, כי כל חזקה אחרת תמפה למספר כלשהו ומספר צריך למפות לעצמו, ולכן כל אוטומורפיזם צריך להעלות כל איבר בחזקה j כאשר קיים $n \in \mathbb{N}$ המקיים $j = np$). $\square$

סעיף ב'

תהיי L/K הרחבה סופית ויהי $L)$overline$($ סגור אלגברי של L. אם שני איברים $\alpha, \beta \in \overline{L}$ צמודים מעל K אז הם גם צמודים מעל L.

הוכחה: הטענה **לא נכונה**.

ניקח $K = \mathbb{R}, L = \mathbb{C}$, זו הרחבה אלגברית סופית כי $\mathbb{C} = \mathbb{R}(i)$.

אנחנו יודעים ש־$\pm i$ הם השורשים של הפולינום $x^2 + 1$ מעל $\mathbb{R}$ ולכן הם צמודים.

מצד שני, כל הצמדה היא טריוויאלית מעל $\mathbb{C}$ ולכן $\pm i$ לא צמודים מעל $\mathbb{C}$.

זאת בערך הטענה ההפוכה מהמועד א'. $\square$

סעיף ג'

תהיי E/K הרחבת שדות ויהיו L, F תתי־הרחבות כך ש־$E = LF$. אם L/K סופית אז E/F סופית.

הוכחה: הטענה **נכונה**.

L/K סופית ולכן לפי תנאים שקולים לסופיות L/K אלגברית וקיימים $\alpha_1, \cdots, \alpha_n$ אלגבריים מעל K כך שמתקיים $L = K(\alpha_1, \cdots, \alpha_n)$.
אבל אז מהגדרת הקומפוזיטום, $E = F(\alpha_1, \cdots, \alpha_n)$ שאם הם אלגבריים מעל K אז הם גם אלגבריים מעל F וזה התנאי השקול שאומר ש־E/F סופית. $\square$

סעיף ד'

לכל חבורה סופית G ולכל ראשוני $p > 0$ יש הרחבת גלואה L/K של שדות ממציין p כך ש־$G \simeq \mathrm{Gal}(L/K)$.

הוכחה: לא יודעת? $\square$

סעיף ה'

אם להרחבת גלואה סופית לא טריוויאלית L/K אין תתי־הרחבות $K \subsetneq F \subsetneq L$ אז $[L : K]$ ראשוני.

הוכחה: הטענה **נכונה**.

ראינו שמתקיים $|\mathrm{Gal}(L/K)| = [L : K]$.

נניח שזה לא מספר ראשוני, אז קיים p ראשוני ו־$n \in \mathbb{N}$ כך שמתקיים $|\mathrm{Gal}(L/K)| = [L : K] = np$.

אז ל־$\mathrm{Gal}(L/K)$ יש תת־חבורה H מגודל p.

ממשפט ארטין, $F = L^H$ נקבל ש־L/F גלואה ו־$[F : K] = p$, אבל זה אומר ש־F/K היא תת־הרחבה לא טריוויאלית ואמרנו שאין לה תתי־הרחבות לא טריוויאליות. $\square$

שאלה 4

נמצא את שדה הפיצול של $t^8-1\in\mathbb{F}_7[t]$ מעל $\mathbb{F}_7$.

פתרון: אנחנו רוצים להרחיב את $\mathbb{F}_7$ כדי ששורש יחידה פרימיטיבי מסדר 8 יהיה בו, אז חייב להתקיים ש־8 מחלק את הסדר של החבורה הכפלית שהיא מסדר 7^n-1, אז נמצא את ה־n המינימלי כך ש־$8\mid 7^n-1$

$$7^1-1\underset{\bmod 8}{\equiv}6,\ 7^2-1=48\underset{\bmod 8}{\equiv}0$$

ולכן שדה הפיצול הוא $\mathbb{F}_{49}$. $\square$

שאלה 5

יהי $f(t)\in K[t]$ פולינום ספרבילי ופריק ממעלה 4 כך ששדה הפיצול שלו מקיים $[L:K]=4$.

סעיף א'

נמצא את $\mathrm{Gal}(f)$.

הוכחה: f פריק, ולכן קיימים g,h כך שמתקיים $f=gh$, נשים לב שיש רק 2 אופציות לקומבינציית דרגות: או שהדרגה של שניהם היא 2 או של אחד מהם היא 1 ושל השני 3.

בלי הגבלת הכלליות, $\deg(h)=3,\deg(g)=1$ אבל אז $6 \mid [L:K]=4$ וזו כמובן סתירה ולכן $\deg(f)=\deg(g)=2$.

g,h חייבים להיות אי־פריקים (אחרת דרגת ההרחבה תהיה קטנה מ־2).

אנחנו יודעים $\mathrm{Gal}(f)=\mathrm{Gal}(L/K)\leq S_4$ ו־$|\mathrm{Gal}(f)|=4$, יש ל־S_4 שתי תתי־חבורות מסדר 4 והן C_4,V כאשר V חבורת קליין.

אבל $f=(t^2+a_1t+b_1)(t^2+a_2t+b_2)$ כאשר השורשים הם בלתי־תלויים ולכן כל פולינום כזה מביא לנו הרחבה מדרגה 2 ולכן $\mathrm{Gal}(f)=C_2\times C_2=V$. $\square$

סעיף ב'

נמצא דוגמה לפולינום כזה כאשר $K=\mathbb{F}_2(x)$.

הוכחה: ניקח (t^2+t+1) אנחנו יודעים שהוא אי־פריק מעל $\mathbb{F}_2(x)$ כי אין לו שורש והוא ספרבילי כי $\gcd(t^2+t+1,2t+1)\underset{\mathrm{mod}\,2}{\equiv}\gcd(t^2+t+1,1)=1$. וניקח (t^2+t+x) שהוא אי־פריק כי אין לו שורש מעל $\mathbb{F}_2$ והוא גם ספרבילי כי $\gcd(t^2+t+x,2t+1)\underset{\mathrm{mod}\,2}{\equiv}\gcd(t^2+t+x,1)=1$. אז $f(t)=(t^2+t+1)(t^2+t+x)$ מסיים. $\square$