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

19 ביולי 2025

שאלה 1

אם L שדה ו־$G \subset \mathrm{Aut}(L)$ תת־חבורה סופית אז L היא הרחבת גלואה סופית של $K = L^G$ ו־$G = \mathrm{Gal}(L/K)$.

הוכחה: אין לי כח לכתוב הוכחה מסודרת, סליחה :-($\square$

שאלה 2

הרחבת שדות L/K היא סופית אם ורק אם היא אלגברית ונוצרת סופית.

הוכחה:

$\Longleftarrow$ נניח שהרחבה סופית ונרצה להראות שהיא אלגברית ונוצרת סופית.

מהסופיות מתקיים (מהגדרה)

$$\alpha \text{ אלגברי מעל } K \Longleftrightarrow [K(\alpha):K]<\infty$$

ולכן זו הרחבה אלגברית (בפרט לכל $\alpha\in L$ מתקיים $[K(\alpha):K]\le[L:K]$) ולכן $[L:K]=n$ אז $\alpha_1,\cdots,\alpha_n$ זה בסיס של L מעל K ולכן $L=K(\alpha_1,\cdots,\alpha_n)$ ולכן L נוצרת סופית מעל K.

$\Longrightarrow$ נניח שהיא אלגברית ונוצרת סופית ונרצה להראות ש־$[L:K]<\infty$.

אם L/K נוצרת סופית ואלגברית אז יש יש לה קבוצת יוצרים $\alpha_1,\cdots,\alpha_k$ והיות וההרחבה אלגברית בפרט $\alpha_1,\cdots,\alpha_k$ אלגבריים.

נסמן $n_1,\cdots,n_k$ הדרגות של $\alpha_1,\cdots,\alpha_k$ בהתאמה, עלינו להראות $[L:K]\le n_1n_2\cdots n_k$.

לכל $1\le i\le k$ נסמן $L_i=K(\alpha_1,\cdots,\alpha_i)$ וכן $L_0=K$, נשים לב כי אם מתקיים $[L_i:L_{i-1}]\le n_i$ אז מכפליות הדרגה נקבל

$$[L:K]=[L_k:L_{k-1}]\cdot[L_{k-1}:L_{k-2}]\cdot\cdots\cdot[L_2:L_1]\cdot[L_1:L_0]\le n_k\cdot n_{k-1}\cdot\cdots\cdot n_2\cdot n_1$$

נזכר ש־$[L_i:L_{i-1}]$ זו הדרגה של הפולינום המינימלי g_i של α_i מעל L_{i-1}, אבל $m_{\alpha_i}(x)$ הוא הפולינום המינימלי של α_i מעל K הוא בפרט פולינום מעל השדה L_{i-1} (שמכיל את K) ומתקיים $g_i\mid m_{\alpha_i}$ ובפרט $[L_i:L_{i-1}]=\deg(g_i)\le\deg\left(m_{\alpha_i}\right)=n_i$. $\square$

שאלה 3

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

סעיף א'

אם K שדה ממציין $p>0$ אז ההעתקה $f: K \to K$ המוגדרת על־ידי $f(x) = x^{p^3}$ היא אנדומורפיזם (הומומורפיזם מ־K לעצמו).

הוכחה: הטענה **נכונה** (זו בעצם הרצה שלישית של הפרבוניוס הרגיל שאנחנו מכירים). עלינו להראות:

1. $f(x+y) = f(x) + f(y)$
2. $f(xy) = f(x)f(y)$
3. $f(1) = 1$

אנחנו בשדה ממציין p אז מתקיים $(x+y)^p = x^p + y^p$ ובאופן כללי $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ (נובע מהבינום, כי כל $\binom{p^k}{k}$ עבור $0<k<p^n$ מתחלק ב־p).

אז

1. $f(x+y) = (x+y)^{p^3} = x^{p^3} + y^{p^3} = f(x) + f(y)$
2. $f(xy) = (xy)^{p^3} = x^{p^3}y^{p^3} = f(x)f(y)$
3. $f(1) = 1^{p^3} = 1$

אז זה אכן אנדומורפיזם (בניגוד לאנדומורפיזם של פרובניוס, אנחנו לא יודעים אם הוא חד־חד ערכי, והוא כנראה אפילו לא ללא התנייה נוספת). □

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 הרחבת גלואה סופית אז $(LF)/F$ גלואה סופית.

הוכחה: הטענה **נכונה**.

מכיוון ש־L/K הרחבת גלואה סופית אז היא גם סופית (דה), גם נורמלית וגם ספרבילית. נשים לב

1. ההרחבה LF/F סופית: זה נובע מכך ש־L/K סופית ו־F/K היא הרחבה אלגברית (כי $F \subseteq \overline{K}$) אז הקומפוזיטום שלנו סופי, כי
$$[LF:F] \underset{\text{תרגיל 17.34 בספר}}{\leq} \underbrace{[L:K]}_{<\infty} \cdot \underbrace{[F:F]}_{=1} < \infty$$
2. ההרחבה LF/F ספרבילית: L/K ספרבילית אז כל האיברים של L ספרביליים מעל כל שדה ביניים, ו־$F \subseteq \overline{K}$ (כי הספרביליות לא תלויה בשדה ההרחבה), אז $\alpha \in \overline{K}$ ספרבילי מעל K אז הוא גם ספרבילי בכל $K \subseteq F \subseteq \overline{K}$
3. ההרחבה LF/F נורמלית – זה למה 36 מסיכומי התרגולים

□

סעיף ג'

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

הוכחה: הטענה **לא נכונה**.

ראינו בהרצאה שכל שדה סופי הוא פרפקטי ובשדה פרפקטי כל הרחבה אלגברית היא הרחבה ספרבילית.

הרחבה מדרגה p היא הרחבה סופית ומהתנאים השקולים להרחבות סופיות נובע שההרחבה היא אלגברית ועל־כן פרידה. □

סעיף ד'

כל הרחבה נורמלית וסופית $K/\mathbb{Q}$ היא גלואה.

הוכחה: הטענה **נכונה**.

אם ההרחבה סופית זה אומר שהיא נוצרת סופית ואלגברית (תנאים שקולים לסופיות) והיא נורמלית, אז כל פולינום אי־פריק מעל $\mathbb{Q}$ מתפצל לגורמים לינאריים ב־K, ואנחנו יודעים שכל הרחבה סופית מעל $\mathbb{Q}$ היא ספרבילית כי אנחנו בשדה ממציין 0 ובשדה ממציין 0 כל פולינום מינימלי הוא ספרבילי.

אז ההרחבה היא נורמלית וספרבילית ולכן גלואה. □

שאלה 4

יהי K שדה ו־$\alpha, \beta \in \overline{K}$ איברים אלגבריים מעל K.
נוכיח שמתקיים

$$[K(\alpha, \beta) : K] \leq [K(\alpha) : K] \cdot [K(\beta) : K]$$

הוכחה: $\alpha, \beta \in \overline{K}$ הם אלגבריים מעל K ולכן ההרחבות $K(\alpha)/K, K(\beta)/K$ הן הרחבות אלגבריות נוצרות סופית ולכן סופיות (מהתנאים השקולים).
אז ממגדל הרחבות

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K]$$
$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\beta)] \cdot [K(\beta) : K]$$

היות ו־β אלגברי מעל K הוא בפרט אלגברי מעל $K(\alpha)$ ולכן ההוספה של β יכולה לכל היותר להשאיר את הדרגה במקום או להקטין אותה (אותם שיקולים תקפים גם עבור α), אז

$$[K(\alpha, \beta) : K(\alpha)] \leq [K(\beta) : K]$$
$$[K(\alpha, \beta) : K(\beta)] \leq [K(\alpha) : K]$$

ובסך־הכל נקבל

$$[K(\alpha, \beta) : K] \leq [K(\alpha) : K] \cdot [K(\beta) : K]$$

$\square$

שאלה 5

נמצא דוגמה להרחבת שדות לא נורמלית L/K כך שמתקיים $[L:K]=4$ ונחשב את $\operatorname{Aut}(L/K)$.

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

הפולינום x^4-2 אי־פריק מעל $\mathbb{Q}$ מקריטריון אייזנשטיין ולכן $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$.

נראה שההרחבה לא נורמלית, מספיק שנראה שלא כל השורשים של הפולינום x^4-2 נמצאים ב־L ולכן הוא לא יתפצל לחלוטין.

אנחנו יודעים שהשורשים של x^4-2 ב־$\overline{\mathbb{Q}}$ הם $\alpha,-\alpha,i\alpha,-i\alpha$ (אפשר לראות את זה גם בגלל ש־$x^4-2=\prod_{k=0}^{3}\left(x-i^k\sqrt[4]{2}\right)$) אבל כמובן ש־$i\notin L\subset\mathbb{R}$ אז הפולינום לא מתפצל לחלוטין ולכן ההרחבה שלנו לא נורמלית.

ניזכר $\operatorname{Aut}(L/K)$ זו חבורת כל האוטומורפיזמים של L שמשמרים את $\mathbb{Q}$, ושולחים כל α לשורש אחר של הפולינום המינימלי שלנו. נשים לב שהשורשים היחידים שנמצאים בהרחבה הם $\alpha,-\alpha$ ולכן $\sigma\mapsto-\alpha$ הוא האוטומורפיזם היחידי האפשרי מלבד הזהות אז

$$\operatorname{Aut}(L/K)=\{\mathrm{id},\alpha\mapsto-\alpha\}$$

יש לנו בידיוק חבורה אחת מסדר 2 אז $\operatorname{Aut}(L/K)\cong\mathbb{Z}/2\mathbb{Z}$. $\square$

שאלה 6

נניח ש־K שדה ממציין 0 המכיל שורש יחידה פרימיטיבי מסדר 3.

נוכיח שההרחבה $K\left(\sqrt{2}+\sqrt[3]{3}\right)/K$ היא ציקלית.

הוכחה: לנוחות נסמן $L=K\left(\sqrt{2}+\sqrt[3]{3}\right)$, ובגלל ש־$\mathrm{char}(K)=0$ אז $\mathbb{Q}\subseteq K$.

נגיד שההרחבה L/K היא **ציקלית** אם ההרחבה היא גלואה (ועל־כן, נורמלית וספרבילית) ואם $G=\mathrm{Gal}(L/K)$ היא ציקלית.

ההרחבה L/K היא הרחבה סופית: נשים לב ש־$\sqrt[3]{3}\notin K\left(\sqrt{2}\right)$ (כי כל איבר ב־$K\left(\sqrt{2}\right)$ הוא מהצורה $a+b\sqrt{2}$ עבור $a,b\in K$), אז הפולינום x^3-3עדיין אי־פריק מעל $K\left(\sqrt{2}\right)$ אז $\left[K\left(\sqrt[3]{3},\sqrt{2}\right):K(2)\right]=3$ ואז מכפליות הדרגה

$$\left[K\left(\sqrt[3]{3},\sqrt{2}\right):K\right]=\left[K\left(\sqrt[3]{3},\sqrt{2}\right):K\left(\sqrt{2}\right)\right]\cdot\left[K\left(\sqrt{2}\right):K\right]=3\cdot 2=6$$

L/K היא הרחבה ספרבילית: נזכר שבמציין 0, כל הרחבה אלגברית היא הרחבה ספרבילית.

נשים לב ש־$\sqrt{2}$ הוא אלגברי מעל $\mathbb{Q}$ כי הוא השורש של הפולינום x^2-2, ו־$\sqrt[3]{3}$ הוא גם אלגברי מעל $\mathbb{Q}$ כי הוא השורש של הפולינום x^3-3.

אז $\sqrt[3]{3},\sqrt{2}$ אלגבריים מעל $\mathbb{Q}$ ו־$\mathbb{Q}\subseteq K$ אז בפרט $\alpha=\sqrt{2}+\sqrt[3]{3}$ הוא אלגברי מעל K (סכום של איברים אלגבריים הוא אלגברי, זה נובע משאלה 4 ישירות).

אז ההרחבה אלגברית ולכן היא ספרבילית.

ההרחבה L/K היא הרחבה נורמלית: מהתנאים השקולים לנורמליות, מספיק שנראה ש־L הוא שדה פיצול של פולינום כלשהו ב־$K[x]$, כלומר שכל השורשים שלו נמצאים.

יש לנו את הפולינומים x^2-2,x^3-3 ועלינו להראות שכל השורשים שלהם נמצאים בהרחבה שלנו.

נסמן $\alpha=\sqrt[3]{3},\beta=\sqrt{2}$ והצמודים שלהם הם $\alpha,\xi_3\alpha,\xi_3^2\alpha,\beta,-\beta$ אז כל ההצמדות של $\theta=\alpha+\beta$ הם

$$\left\{\alpha+\beta,\xi_3\alpha+\beta,\xi_3^2\alpha+\beta,\alpha-\beta,\xi_3\alpha-\beta,\xi_3^2\alpha-\beta\right\}$$

אז בפרט $K(\theta)\subseteq K(\alpha,\beta)$ נשים לב שאנחנו לא יכולים לבחון בצורה נוחה את $K\left(\sqrt[3]{3}+\sqrt{2}\right)$ כי זה לא יוצר את כל ההרחבה $K\left(\sqrt[3]{3},\sqrt{2}\right)$ אבל $\sqrt[3]{3}+\sqrt{2}\in K\left(\sqrt[3]{3},\sqrt{2}\right)$. ונגדיר $H:=K\left(\sqrt[3]{3},\sqrt{2}\right)=K$ (ממשפט האיבר הפרימיטיבי θ יוצר אחר־כך את ההרחבה אז זה שקול, אבל אנחנו צריכים הפרדה לשורשים כדי לחקור את מה שחבורת גלואה עושה לשורשים) זו הרחבה כמובן מדרגה 6 כפי שראינו מקודם אז השורשים יוצרים בסיס עם שישה איברים

$$\left\{1,\beta,\alpha,\beta\alpha,\alpha^2,\beta^2\right\}$$

כעת, היות ו־$\sqrt{2}\in H$, אז $\sqrt[3]{3}+\left(\sqrt{2}+\sqrt[3]{3}\right)-=-\sqrt{2}$ ולכן כל השורשים של x^2-2 נמצאים ב־H.

בנוסף, $\sqrt[3]{3}\in H$ ו־$\xi_3\in K$ אז $\xi_3\sqrt[3]{3},\xi_3^2\sqrt[3]{3}\in H$ ולכן גם כל השורשים של x^3-3 נמצאים ב־H.

אז כל השורשים של הפולינומים האי־פריקים שלנו נמצאים בהרחבה, אז בעצם הוא מתפצל לחלוטין בהרחבה שלנו ולכן ההרחבה שלנו נורמלית.

הערה: כל המהלך על הבסיס מיותר נעה...

אז יש לנו הרחבה ספרבילית, סופית ונורמלית ולכן ההרחבה H/K היא הרחבת גלואה, ולא רק שהיא הרחבת גלואה מדרגה 6.

אנחנו יודעים שיש בידיוק 2 חבורות מסדר 6 והן $S_3,\mathbb{Z}_6$. בגלל ש־$\sqrt{2},\sqrt[3]{3}$ הם אלגבריים מעל K והם מהווים שורשים של פולינומים אי־פריקים שונים מעל K (ואפילו אין שורש משותף ביניהם), אז אין תלות לאן האוטומורפיזם שולח את השורש (כי כל אוטומורפיזם משמר את K ועושה פרמוטציות על השורשים של הפולינומים האי־פריקים), אז $\sqrt{2}$ נשלח אל $\pm\sqrt{2}$ ו־$\sqrt[3]{3}$ נשלח אל אחד מ־$\left\{\sqrt[3]{3},\xi_3\sqrt[3]{3},\xi_3^2\sqrt[3]{3}\right\}$ וכל שליחה לא משפיעה על השנייה, אז יש לנו 6 אוטומורפיזמים (2ל־$\sqrt{2}$ ו־3 ל־$\sqrt[3]{3}$), אז בעצם חבורת גלואה נוצרת על־ידי שני יוצרים – אחד מסדר 2 ואחד מסדר 3, וזה בידיוק

$$\mathrm{Gal}(H/K)=\mathrm{Gal}\left(K\left(\sqrt{2},\sqrt[3]{3}\right)\right)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\underset{\text{משפט השאריות הסיני}}{\cong}\mathbb{Z}_6$$

שהיא באמת ציקלית כמו שרצינו. $\square$

שאלה 7

יהי $p > 2$ ראשוני ו־K שדה פיצול של הפולינום $x^8 - 1$ מעל $\mathbb{F}_p$. נוכיח ש־$\left[K : \mathbb{F}_p\right] \leq 2$.

הוכחה: הפולינום $x^8 - 1$ מתפצל לחלוטין מעל כל שדה שמכיל את שורש יחידה מסדר 8, אז מהגדרה של K כשדה פיצול של הפולינום נובע שזו ההרחבה המינימלית של $\mathbb{F}_p$ שמכילה את כל שמונת שורשי היחידה, זה בידיוק $K = \mathbb{F}_p(\mu_8)$ (μ_8 זו קבוצת כל שורשי היחידה משורש 8 ב־$\overline{\mathbb{F}_p}$).

ניזכר ש־$\mathbb{F}_{p^n}^{\times}$ היא ציקלית מסדר $p^n - 1$ והיא מכילה את כל שורשי היחידה מסדר 8 אם ורק אם $8 \mid (p^n - 1)$ כלומר אם ורק אם $p^n \underset{8}{\equiv} 1$.

האופציות היחידות ל־p הן $\{1, 3, 5, 7\}$ וכמובן 1 נפסל מההנחה, נחשב ידנית

$$p = 3 \Rightarrow p^2 = 9 \underset{\bmod 8}{\equiv} 1$$

$$p = 5 \Rightarrow p^2 = 25 \underset{\bmod 8}{\equiv} 1$$

$$p = 7 \Rightarrow p^2 = 49 \underset{\bmod 8}{\equiv} 1$$

אז כל שורשי היחידה מסדר 8 נמצאים כבר ב־$\mathbb{F}_{p^2}$ ולכן $K \subseteq \mathbb{F}_{p^2}$ אז בפרט בגלל היחס בין הכלה לבין דרגות

$$\left[K : \mathbb{F}_p\right] \leq \left[\mathbb{F}_{p^2} : \mathbb{F}_p\right] \leq 2$$

כאשר הדרגה של האחרון היא 2 כי אם נסמן α הוא שורש של פולינום אי־פריק מדרגה 2, אז כל איבר ב־$\mathbb{F}_{p^2}$ הוא מהצורה $a + b\alpha$ עבור $a, b \in \mathbb{F}_p$ כי $\{1, \alpha\}$ הוא בסיס:

1. בלתי־תלוי לינארית כי אם לא, אז עבור $a, b \in \mathbb{F}_p$ מתקיים $\alpha = -\frac{a}{b} \underset{b \neq 0}{\iff} a + b\alpha = 0$ אבל אמרנו ש־α הוא שורש של פולינום אי־פריק מדרגה 2 מעל $\mathbb{F}_p$, אז ברור שזה לא אפשרי אז רק הפיתרון הטריוויאלי תופס
2. זה פורש כי כל איבר ב־$\mathbb{F}_{p^2}$ הוא מהצורה $c_0 + c_1\alpha$ עבור $c_0, c_1 \in \mathbb{F}_p$, אבל α הוא שורש של פולינום אי־פריק מדרגה 2 והוא יוצר את ההרחבה אז בוודאי שניתן לכתוב כל איבר באמצעות צירוף שלו

$\square$