

אלגברה ב' 2 – תרגול 12

6.6.11

הרחבות טרנסצנדנטיות

תהי L/K הרחבה של שדות. $T \subseteq L$ תקרא ב"ת אלגברית מעל K אם לכל $t_1, \dots, t_n \in T$ שונים, $n \in \mathbb{N}$ ולכל $0 \neq f \in K[x_1, \dots, x_n]$ $f(t_1, \dots, t_n) \neq 0$. ראינו שבמקרה זה כל $t \in T$ הוא טרנסצנדנטי מעל K . $T \subseteq L$ נקראת בסיס טרנסצנדנטי של L מעל K אם $L/K(T)$ אלגברית ו- T ב"ת אלגברית- K . באופן שקול אם T מרבית ב"ת אלגברית- K . ואז מעלת הטרנסצנדנטיות של L/K היא $|T|$. (וראינו שלכל בסיס טרנסצנדנטי יש אותה העוצמה).

דוגמאות. אם $t_1, \dots, t_n$ משתנים, $\mathbb{C}(t_1, \dots, t_n)$ טרנסצנדנטית ממעלה n . π, e טרנסצנדנטיים מעל $\mathbb{Q}$. השערה π, e ב"ת אלגברית מעל $\mathbb{Q}$.

שאלה. הוכיחו כי ל- $\mathbb{C}$ יש $2^{\aleph}$ אוטומורפיזמים.

הערה. אנחנו מכירים שני אוטומורפיזמים: הזהות וההצמדה. הם היחידים שרציפים ובדר"כ היחידים שמעניינים. אם φ אוטומורפיזם אז $\varphi|_{\mathbb{Z}} = id_{\mathbb{Z}}$ לכן הזהות גם על $\mathbb{Q}$. אז $\varphi(i^2) = \varphi(-1) = -1$ לכן $\varphi(i) = \pm i$. קבענו את φ על $\mathbb{Q}[i]$, קבוצה צפופה ב- $\mathbb{C}$ ומרציפות זאת או ההצמדה או הזהות.

פתרון. שלב הראשון: נראה שאם יש בסיס טרנסצנדנטי ל- $\mathbb{C}/\mathbb{Q}$ מעוצמה β אז יש לפחות 2^β אוטומורפיזמים. נבחין כי אוטומורפיזם כנ"ל הוא בהכרח מעל $\mathbb{Q}$ כלומר קובע את $\mathbb{Q}$ במקום. נראה שמספר האוטומורפיזמים מעל $\mathbb{Q}$ הוא 2^β . יהי T בסיס טרנסצנדנטי. נכתוב $T = T_0 \cup T_1$ נגדיר $T'_1 = \{-t : t \in T_1\}$, $T'_1 = \{-t : t \in T_1\}$. אפשר להגדיר פונקציה $\varphi : T \rightarrow T'$ ע"י

$$\varphi(t) = \begin{cases} t & t \in T_0 \\ -t & t \in T_1 \end{cases}$$

גם T' הוא בסיס טרנסצנדנטי: ברור כי T' ב"ת אלגברית מעל $\mathbb{Q}$ ו- $\mathbb{Q}(T') = \mathbb{Q}(T)$ לכן $\mathbb{C}/\mathbb{Q}(T')$ אלגברית ($\mathbb{C}/\mathbb{Q}(T)$ אלגברית). נרחיב את φ ביחידות להומומורפיזם מ- $\mathbb{Q}[T] \rightarrow \mathbb{Q}[T']$ ועדיין נקרא לו φ . כעת נרחיב ביחידות להומומורפיזם של שדה המנות $\varphi : \mathbb{Q}(T) \rightarrow \mathbb{Q}(T')$.

לכן φ ניתן להרחבה להומומורפיזם $\varphi : \mathbb{C} \rightarrow \mathbb{C}$. כפונקציה מ- $T \rightarrow T'$ הפיכה ולכן גם $\varphi : \mathbb{C} \rightarrow \mathbb{C}$ הפיכה.

ברור כי כל חלוקה של T ל- T_0, T_1 כנ"ל משרה אוטומורפיזם אחר. שלב שני: מעלת הטרנסצנדנטיות היא $\aleph$. יהי T כמו בשלב הראשון. אז הסגור האלגבי של $\mathbb{Q}(T) = \mathbb{C}$ לכן $\aleph = |\overline{\mathbb{Q}(T)}| = |\overline{\mathbb{Q}(T)}|$ אבל $|\overline{\mathbb{Q}(T)}| = |\mathbb{Q}(T)|$ (כי $\overline{\mathbb{Q}(T)}/\mathbb{Q}(T)$ אלגברית) ואז $|\mathbb{Q}(T)| \leq |\overline{\mathbb{Q}(T)}| \leq \max\{|\mathbb{Q}(T)|, \aleph_0\}$ בנוסף $|\mathbb{Q}(T)| = |T|$ כי אם $|T| < \infty$ אז $|\mathbb{Q}(T)| = \aleph_0$ בסתירה, ואז $|T|$ אינסופית ולכן $|\mathbb{Q}(T)| = |T|$. משני השלבים יש $2^{\aleph} \leq$ אוטומורפיזמים אבל יש $2^{\aleph}$ פונקציות מ- $\mathbb{C} \rightarrow \mathbb{C}$ ולכן יש בדיוק $2^{\aleph}$ אוטומורפיזמים. אין כל כך מה לעשות איתם, אבל הם שם.

הערה. בתרגיל בית מצאנו את $\overline{\mathbb{Q}} \subset \mathbb{C}$ ובכל זאת $\overline{\mathbb{Q}} \subsetneq \mathbb{C}$ בניגוד לטעיון ש-
 $\overline{\mathbb{Q}(T)} = \mathbb{C}$ בפתרון. ההסבר הוא ש- $\mathbb{C}/\mathbb{Q}$ איננה אלגברית בניגוד ל- $\mathbb{C}/\mathbb{Q}(T)$.

שאלה. תהי L/K הרחבה המקיימת:

1. L סגור אלגברית.

2. מעלת הטרנסצנדנטיות של L/K סופית.

1. יהי $\varphi : L \rightarrow L$ הומומורפיזם- K . צ"ל φ אוטומורפיזם.

פתרון. יהי $T \subseteq L$ בסיס טרנסצנדנטי. אז $|\varphi(T)| = |T|$. אז $\varphi(T)$ ב"ת אלגברית- K , כי אם $t_1, \dots, t_n \in T$ שונים ו- $f \in K[x_1, \dots, x_n]$ כך $0 \neq f(t_1, \dots, t_n) = 0$ ש- $\varphi(f(t_1, \dots, t_n)) = f(\varphi(t_1), \dots, \varphi(t_n)) = 0$ בסתירה. מהנתון השני $\varphi(T)$ בסיס טרנסצנדנטי של L/K כי אחרת ניתן להרחיב את $\varphi(T)$ ולקבל בסיס בעוצמה גדולה ממש מהעוצמה של T בסתירה.

אז $L/K(\varphi(T))$ אלגברית. בנוסף $K(\varphi(T)) \subset \varphi(L) \subset L$ לכן אם נראה $\varphi(L)$ סגור אלגברית אז $L = \varphi(L)$. יהי $L = \varphi(L)$ יהי $g = \sum_{i=0}^n \alpha_i x^i \in \varphi(L)[x]$ $\deg g \geq 1$. יש $\beta_i \in L$ כך ש- $\varphi(\alpha_i) = \beta_i$ $\tilde{g} = \sum_{i=0}^n \beta_i x^i \in L[x]$ ממעלה לפחות 1. יהי $y \in L$ שורש של $\tilde{g}$ אז $\varphi(y) \in \varphi(L)$ שורש של g .

2. האם שני הנתונים הכרחיים?

פתרון. כן. למשל $\mathbb{C}(x) \rightarrow \mathbb{C}(x)$, $x \mapsto x^2$ משתנה, $\varphi : x \mapsto x^2$ איננו איזומורפיזם. $K = \mathbb{C}$, $L = \mathbb{C}(x)$ והתנאי הראשון לא מתקיים השני כן.

למקרה השני ניקח $K = \mathbb{C}$, $L = \overline{\mathbb{C}(\{x_i : i \in \mathbb{N}\})}$, $\varphi : x_i \mapsto x_{i+1}$ איננו איזומורפיזם. התנאי השני לא מתקיים, הראשון כן.

הערה. $\mathbb{C}(x) \xrightarrow[\mathbb{C}]{\sim} \mathbb{C}(x^2)$ ע"י $x \mapsto x^2$.

הערה. הרחבה L/K היא אבלית/מעגלית אם L/K גלואה וגם $\text{Gal}(L/K)$ היא אבלית/מעגלית.

הרחבה L/K פתירה אם יש $\tilde{L}/K$ כך ש- $L \subset \tilde{L}$, $\tilde{L}/K$ גלואה ו- $\text{Gal}(\tilde{L}/K)$ פתירה. כי הגדרנו הרחות $\mathcal{C}$ עבור משפחה של חבורות סופיות, מלאה, חבורות אבליות מעגליות אינן מהוות משפחה מלאה).

מבחן 2009, גינזבורג

3.

1. מהי חבורת גלואה של $x^3 - 2$ מעל $\mathbb{Z}_{11}, \mathbb{Z}_5$?

פתרון. $x^3 - 2 = (x+2)(x^2 - 2x - 1)$ מעל $\mathbb{Z}_5$. שדה הפיצול L ממעל 2 מעל $\mathbb{Z}_5$.

לכן $\text{Gal}(L/\mathbb{Z}_5) \approx \mathbb{Z}_2$. מעל $\mathbb{Z}_{11}$ $x^3 - 2 = (x-7)(x^2 + 7x + 5)$ מעל $\mathbb{Z}_{11}$ $x^3 - 2 = (x-7)(x^2 + 7x + 5)$ מעל $\mathbb{Z}_{11}$.

2. תהי $F/\mathbb{Q}$ גלואה ממעלה 8 ונניח כי כל איבר $e \neq 1$ ב- $G = \text{Gal}(F/\mathbb{Q})$ הוא מסדר

2. מצאו לכמה תתי שדות של F יש מעלה 4 מעל $\mathbb{Q}$. אם $L \subset F$ אז $\mathbb{Q} \subset L \subset F$. תהי $H < G$ כך ש- $L = F^H$.

$$8 = [F : \mathbb{Q}] = \underbrace{[F : L]}_{=|H|} [L : \mathbb{Q}]$$

לכן אם $[L : \mathbb{Q}] = 4$ אז $|H| = 2$. מכיוון שיש 7 ת"ח ל- G בנות 2 איברים אז יש 7 שדות כ"ל.

2003 ירדן

1. הוכיחו או הפריכו:

1. $F_9 \subset F_{27}$.

2. $F_9 \subset F_{81}$.

פתרון. $m \mid n \Leftrightarrow F_{p^m} \subset F_{p^n}$ לכן הסעיף הראשון לא נכון והסעיף השני נכון.

6. הוכיחו ש- $\text{Gal}(x^5 - 4x + 2, \mathbb{Q}) \cong S_5$.

פתרון. הנגזרת $5x^4 - 4$ מתאפסת על 2 הנקודות ממשיות בדיוק $(x = \pm \sqrt{\frac{2}{5}})$ לכן יש בדיוק 3 שורשים שונים ממשיים ולכן מתרגיל בתרגול נקבל S_5 .

ירדן 2010

2. יהי $K = K_0 \subset K_1 \subset \dots \subset K_r$ מגדל של שדות בעלי אפיון 0. נניח שלכל $1 \leq i \leq r$, K_i מתקבל מ- K_{i-1} ע"י הוספת שורש n -י של איבר של K_{i-1} . צ"ל יש הרחבה פתירה $K_r \subset N$.

פתרון. רדיקלית K_i/K_{i-1} (ולכן פתירה) וממשפט בשיעור על הרחבות C נובע K_r/K_0 תירה ניקח $N = K_r$.

3. מצאו הרחבת גלואה כך ש- $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. תארו את ההרחבה באופן מפורש.

פתרון. לכל A אבלית סופית יש $K/\mathbb{Q}$ גלואה עם $\text{Gal}(K/\mathbb{Q}) \cong A$. לפי הבניה בשיעור ניקח $p_i \equiv 1 \pmod{n_i}$ ראשוניים, $i = 1, 2, \dots$ כאן $p_1 = 7, p_2 = 17$, $L_i = \mathbb{Q}(\xi_{p_i})$, $K_1 = L_1$, $K_2 = L_2^{H_2}$, $K = K_1 K_2$. ניקח $G_i = \text{Gal}(L_i/\mathbb{Q}) \cong (\mathbb{Z}/p_i\mathbb{Z})^* \cong \mathbb{Z}/(p_i-1)\mathbb{Z}$ מעגלית. $H_2 < (\mathbb{Z}/p_2\mathbb{Z})^*$ מאינדקס 8 $(|H_2| = 2)$ ולכן $\text{Gal}(K_2/\mathbb{Q}) \cong \mathbb{Z}/8\mathbb{Z}$. ומאוחות המשפט $\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. אם רוצים אז אפשר להמשיך: H_2 נבחרת כך, ניקח $H_2 = \langle \sigma^8 \rangle$, $id \neq \sigma \in \text{Gal}(L_2/\mathbb{Q})$.

2003 ירדן.

3. יהי K שדה אינסופי, $x, y \in \bar{K}$ כך ש- y פריד מעל K . צ"ל $\exists z \in K(x, y). K(z) = \bar{K}$.

פתרון. יהיו $f, g \in K[x]$ הפולינומים הא"פ של x, y בהתאמה $(f(x) = 0)$. יהיו $x = y_1, \dots, y_n, x_1, \dots, x_m \in \bar{K}$ כל השורשים הושינים של f ושל g . נגדיר $\tilde{K}(T) \ni Q(T) = \prod_{i,j,k,l} (x_i + Ty_i - (x_k + Ty_l))$ כך ש- $(i, j) \neq (k, l)$

זה לא פולינום האפס. כל גורם במכפלה הוא מהצורה $T(y_j - y_l) + (x_i - x_k) \neq 0$ כפולינום ב- $\tilde{K}[T]$. מכיון ש- K אינסופי יש $a \in K$ כך ש- $Q(a) \neq 0$. אז לכל $Q(a) \neq 0$ $(i, j) \neq (k, l)$ ובפרט $x_i + ay_j \neq x_k + ay_l$ לכל $l > 1$, $z = x + ay$ נוסח $z \in K(z)$ נוכיח $y \in K(z)$ ואז ברור מכיון ש- $a \in K$ שגם $x \in K(z)$. כנדרש.

נגדיר $h(S) = f(z - aS) \in K(z)[S]$. מצד שני, $h(y) = f(z - ay) = f(x) = 0$. $h(S) = f(z - aS) \in K(z)[S]$ השורש היחיד ל- $h(y_l) = f(z - ay_l) = f(x + ay - ay_l) \neq 0$, $l > 1$ לכל $h(y_l) \neq 0$, $l > 1$ $k \geq q$. $(S - y)^a = \gcd(h(S), g(S))$ $a \geq 1$ לכן עבור $x + ay - ay_l \neq x_k$. אבל $a = 1$ כי y פריד, כלומר כל שורשי g שונים. $K(z)[S] \ni \gcd(h(S), h(S)) = S - y$.