

אלגברה ב' 2 – הרצאה 26

1.6.11

תרגיל. תהי T ב"ת אלגברית מעל שדה K . אם $\alpha \in K(T)$ ו- α אלגברי מעל K , אז $\alpha \in K$.

הוכחה. $\alpha = \frac{g(t)}{h(t)}$, $g, h \in K[x_1, \dots, x_n]$ ו- t ניה של איברי T , $h(t) \neq 0$. בה"כ $g(t) \neq 0$ (כי אחרת $\alpha = 0$). בה"כ g, k זרים $(K[x_1, \dots, x_n])$ הוא תחום פריקות, ואחרת נצמצם). לפי ההנחה (אלגבריות) קיימים $a_0, \dots, a_d \in K$ כך ש- $\sum_{i=0}^d a_i \alpha^i = 0$. בה"כ גם $a_0 \neq 0$ (אחרת נחלק ב- α). נכפיל את השוויון האחרון ב- $h(t)^d$:

$$\sum_{i=0}^d a_i (g(t))^i (h(t))^{d-i} = 0$$

אם $q \in K[x_1, \dots, x_n]$ אי פריק ו- $q|g$ אז q מחלק את כל המחוברים בסכום למעלה חוץ מזה שמופיע בחזקת 0 והוא ולכן חייב לחלק גם אותו ואז $q|h$. באופן סימטרי אם $q|h$ אז $q|g$. אבל g, h זרים ולכן $h, g \in K^*$ ולכן $\alpha \in K$. $\square$

למה. תהי $T \subseteq L$. התנאים הבאים שקולים:

א. T בת"א מעל K מרבית.

ג. T בת"א מעל K ו- $L/K(T)$ אלגברית.

הוכחה. **תזכורת.** הוכחנו שאם T בת"א מעל K ו- $S \subseteq L$ אז S בת"א מעל $K(T) \Leftrightarrow S \cap T = \emptyset$ ו- $T \cup S$ בת"א מעל K .
תהי T בת"א מעל K . אז $L/K(T)$ אינה אלגברית $\Leftrightarrow$ יש $\alpha \in L$ שאינו אלגברי מעל $K(T)$ $\Leftrightarrow$ יש $\alpha \in L$ כך ש- $\{\alpha\}$ בת"א מעל $K(T)$ $\Leftrightarrow$ יש $\alpha \in L$ כך ש- $\alpha \notin T$ ו- $T \cup \{\alpha\}$ בת"א מעל K $\Leftrightarrow T$ בת"א לא מרבית. וזאת השלילה של הסעיף הראשון. $\square$

הגדרה. T שמקיימת אחד התנאים הנ"ל נקראת בסיס טרנסצנדנטיות (ב"ט) של L/K .

משפט. כל שני ב"ט של L/K הם שוי עוצמה.

הוכחה. יהיו S, T שני ב"ט של L/K . מטעמי סימטריה, די להראות ש- $|S| \leq |T|$. נבדיל בין שני מקרים.

S קבוצה סופית. במקרה זה, יהיו $s_1, \dots, s_n \in S$ $n \geq 0$ שונים זה מזה (נשתמש רק בכך ש- $L/K(T)$ אלגברית, ולא בכך ש- T בת"א מעל K). נראה שקיימים $t_1, \dots, t_n \in T$ שונים זה מזה כך ש-

$$T'_n := \{s_1, \dots, s_n\} \cup (T \setminus \{t_1, \dots, t_n\})$$

ניקח $n = |S|$ ונקבל $|S| \leq |T|$. נראה באמת שיש $t_1, \dots, t_n$ כנ"ל. נוכיח באינדוקציה על n .
 $n = 1$: $s_1 \in L$, לכן s_1 אלגברית מעל $K(T)$ ולכן אחרי מכנה משותף יש $t_1, \dots, t_m \in T$ ויש $f \in K[x_1, \dots, x_m, x_{m+1}]$ כן $0 \neq f$ ש- $f(t_1, \dots, t_m, s_1) = 0$. משתנה x_{m+1} מופיע ב- f (כלומר $f \notin L[x_1, \dots, x_m]$) כי אחרת היינו מקבלים ש- T תלויה אלגברית בסתירה להנחה. באופן דומה מופיע לפחות אחד מהמשתנים $x_1, \dots, x_n$, כי אחרת $0 \neq f \in K[x_{m+1}]$, $f(s_1) = 0$ בסתירה לכך ש- S בת"א מעל K . בה"כ נניח שזה x_1 . אז t_1 אלגברי מעל $K(T_1')$ $K(t_2, \dots, t_m, s_1) \subseteq K(T_1')$. מכאן T אלגברית מעל $K(T_1')$. לכן, $K(T_1')(T)$ אלגברית מעל $K(T_1)$ ו- L אלגברית מעל $K(T_1)(T)$ ולכן L אלגברית מעל $K(T_1')$.
 נעשה את הוכחת האינדוקציה.
 $n = 0$: $T'_0 = T$ וזה ברור.
 כעת, אם בנינו T'_{n-1} כך ש- $L/K(T'_{n-1})$ אלגברית אז לפי המקרה הקודם יש $t_n \in T$ כן $T'_{n-1} \subseteq T$ אלגברי מעל $K(T'_n)$ ו- T'_n בת"א מעל K .
 מקרה שני, S אינסופית. כל $t \in T$ הוא ב- L ולכן אלגברי מעל $K(S)$, לכן t אלגברי מעל $K(S_t)$ באשר $S_t \subseteq S$ סופית.

טענה. $S' := \bigcup_{t \in T} S_t = S$.

$S' \subseteq S$. להפך, יהי $\alpha \in S$ אז α אלגברי מעל $K(T)$, ולכן מעל $K(T')$, עבור איזה $T' \subseteq T$ סופית.
 כל $t \in T'$ אלגברי מעל $K(s_t)$ ובפרט מעל $K(S')$ (כי $K(s_t) \subseteq K(S')$). לכן $K(S')(T')$ אלגברי מעל $K(S')$. אבל, α אלגברי מעל $K(S')(T)$ ולכן α אלגברי מעל $K(S')$. לפי התזכורת, $\alpha \in S$ או $\alpha \in S' \cup \{\alpha\}$ תלויה אלגברית מעל K . אבל $S' \cup \{\alpha\} \subseteq S$ בת"א מעל K ולכן $\alpha \in S'$. הוכחנו ש- $S' = S$. בפרט, T אינסופית ו-

$$|S| \leq |T| \cdot \aleph_0 = |T|$$

□

משפט. כל קבוצה בת"א מעל K ב- L ניתן להשלים לב"ט של L/K .

□

הוכחה. הלמה של צורן.

תרגיל. יהיו L, L' שני שדות סגורים אלגברית כך ש- $\text{chr } L = \text{chr } L'$ ו- $\aleph_0 < |L'| = |L|$. אז $L \cong L'$.

הוכחה. יהיו K, K' השדות הראשוניים של L, L' בהתאמה ויהיו T, T' ב"ט של $L/K, L'/K'$ בהתאמה. נראה ש- $|T| = |T'|$. ואכן, $|K| \leq \aleph_0$. לא ייתכן ש- T סופית, כי אז $|K(T)| \leq \aleph_0$ ולכן $|K(T)| \leq \aleph_0$ בנוסף L/K אלגברית ולכן $|L| \leq \aleph_0$. לכן T, T' קבוצות אינסופיות. לכן, עוצמת קבוצת המונומים ב- T היא $|T|$. לכן, $|K(T)| = |T|$ ואפילו $|K(T)| = |T|$ ולכן היות ו- L אלגברית אז $|L| = |T|$. באותו אופן $|L'| = |T'|$ לכן $|T| = |T'|$.

עכשיו $\text{chr } K = \text{chr } L = \text{chr } L' = \text{chr } K'$ ולכן יש איזומורפיזם $\lambda_1 : K' \rightarrow L$. יש התאמה חח"ע $\lambda_2 : T \rightarrow T'$ אז λ_1, λ_2 מגדירות העתקה $\lambda : K[T] \rightarrow K'[T]$ כאשר המקדמים עוברים לפי λ_1 והמשתנים לפי λ_2 . זה איזומורפיזם. איזומורפיזם של חוגים מגדיר איזומורפיזם של שדות המנות $\widehat{K(T)} \rightarrow \widehat{K'(T')}$ וזה נותן איזומורפיזם על הסגורים האלגבריים $\widehat{K(T)} = L$ ו- $\widehat{K'(T')} = L'$. □

ראינו משפט ארטין שרייר:

משפט. אם $\text{chr } K = p$ אז כל הרחבה מעגלית מעלה p היא פהצורה $K(\alpha)$, שורש של $x^p - x - a \in K[x]$. להיפך, (אם α שורש של $x^p - x - a$ אז גם $\alpha + 1$ הוא שורש, ...) $\alpha + p - 1$ שורש ואז אלה כל השורשים שלו).

ככה אנחנו יודעים לבנות הרחבות ממעלה p .
 כיצד בונים הרחבה ממעלה p^2 ?

משפט. נניח $p = \text{chr } K > 0$. תהי L/K מעגלית ממעלה $N := p^n > 1$ אז יש L'/K מעגלית ממעלה p^{n+1} כך ש- $K \subseteq L \subseteq L'$.

הוכחה. נגדיר $L' = L(\alpha)$ באשר α שורש של $f(x) = x^p - x - a \in L[x]$, עבור איזה $a \in L$.

מציאת a : $\text{Gal}(L/K) = \langle \sigma \rangle$ אז $1, \sigma, \sigma^2, \dots, \sigma^{N-1}$ שונים ולכן ממשפט ארטיין הם ב"ת לינארית ככרסטרים מעל L . לכן, $1 + \sigma + \dots + \sigma^{N-1} \neq 0$. כלומר, קיים $\beta' \in L$ כך שאם נציב אותו נקבל 0. אבל זאת בדיוק העקבה, כלומר, $T_{L/K}(\beta') \neq 0$. נסמו $T_{L/K}(\beta - \beta^p) = 0$ נסתכל על $T_{L/K}(\beta) = 1$ ולכן $\beta = \frac{\beta'}{c}$. יהי $K \ni c := T_{L/K}(\beta) \neq 0$.
 $T_{L/K}(\beta) - T_{L/K}(\beta^p) = T_{L/K}(\beta) - T_{L/K}(\beta)^p = 1 - 1 = 0$
 וזה כי $T_{L/K}(\beta) = \sum_i \sigma^i(\beta^p) = \sum_i (\sigma^i(\beta))^p = (T_{L/K}(\beta))^p$
 לפי הגרסא החיבורית של משפט 90 של הילברט יש $a \in L$ כך ש- $a - ra = \beta - \beta^p$.
 קיבלנו $\sigma a - a = \beta^p - \beta$ (*).

טענה. $f(x) = x^p - x - a$ אי פריק מעל L .

הוכחה. נניח שלא. יהי $\alpha \in \tilde{L}$ שורש של f . אז לפי משפט $\alpha \in L$.

$$\begin{aligned} (\sigma\alpha - \alpha)^p - (\sigma\alpha - \alpha) - (\beta^p - \beta) &= (\sigma(\alpha^p) - \alpha^p) - (\sigma\alpha - \alpha) - (\sigma a - a) = \\ &= \sigma(\alpha^p - \alpha - a) - (\alpha^p - \alpha - a) = \sigma(0) - 0 = 0 \end{aligned}$$

לכן $\sigma\alpha - \alpha$ הוא שורש של $f(x) = x^p - x - (\beta^p - \beta)$. אבל גם β שורש שלו. לכן,
 $0 = T_{L/K}(\sigma\alpha) - T_{L/K}(\alpha) = T_{L/K}(\sigma\alpha - \alpha) = 0$. מכאן $0 \leq i < p$, $\sigma\alpha - \alpha = \beta - \beta^p$
 $T(\beta + i) = T_{L/K}(\beta) + T_{L/K}(i) = 1 - N \cdot i = 1$
 וזאת סתירה.
 לבסוף,

$$(\alpha + \beta)^p - (\alpha + \beta) - \sigma a = \alpha^p - \alpha + \beta^p - \beta - \sigma a = a + \beta^p - \beta - \sigma a = 0$$

כלומר $\alpha + \beta$ הוא שורש של $\sigma f = x^p - x - \sigma a$.
 לכן, ניתן להרחיב את $\sigma : L \rightarrow L$ לאיזומורפיזם $\sigma' : L' \xrightarrow{\sim} L'$ כך ש- $\sigma'(\alpha) = \alpha + \beta$.
 אז צ"ל $\text{ord } \sigma' = p^{n+1}$. לכן די להוכיח ש- $(\sigma')^{p^n} \neq 1$. אבל $(\sigma')^{p^n}(\alpha) = \sigma'(\alpha) = \alpha + \beta$.
 $(\sigma')^j(\alpha) = \alpha + \beta + \sigma(\beta) + \dots + \sigma^{j-1}(\beta)$
 $(\sigma')^{p^n} = \alpha + T_{L/K}(\beta) = \alpha + 1 \neq \alpha$
 ולכן $(\sigma')^{p^n} \neq 1$.
 □
 □