אלגברה ב' 2 – הרצאה 10

23.03.11

אנחנו עוסקים בהרחבות נורמליות. יש לנו שדה K, הסגור האלגברי שלו $\tilde{K}$ אם $F \subseteq K[x]$ שדה הפיצול של F בתוך $\tilde{K}$:

$$K(\{\alpha \in \tilde{K} | 0 \neq f \in F, f \text{ שורש של } \alpha\})$$

L/K נורמלית אם אלגברית וכל פולינום $p \in K[x]$ אי פריק שיש לו שורש ב- L מתפצל מעל L.
כלומר, אם $K \subseteq L \subseteq \tilde{K}$ אז לכל $p \in K[x]$ אי פריק אם יש לו שורש ב- L אז כל שורשיו הם ב-L.

משפט. יהיו $K \subseteq L \subseteq \tilde{K}$. התנאים הבאים שקולים:

1. L נורמלית.
2. יש $F \subseteq K[x]$ כך ש- L שדה הפיצול שלה.
3. כל הומומורפיזם – $\sigma : L \to \tilde{K}$ K הוא אוטומורפיזם של L.
4. כל אוטומופריזם – K של $\tilde{K}$ מקיים: $\sigma(L) = L$.

הוכחה. $1 \Rightarrow 2$: נגדיר את $F := \{\text{irr}(\alpha, K) | \alpha \in L\}$. יהי $L' \subseteq \tilde{K}$ שדה הפיצול של F. נראה $L = L'$. לפי הנתון כל $f \in F$ מתפצל מעל L. לכן $L \subseteq L'$. להפך, כל איבר $\alpha \in L$ הוא שורש של פולינום $f \in F$. לכן בפרט $\alpha \in L'$. לכן $L = L'$.
$2 \Rightarrow 3$: σ הוא שיכון (כל אוטומורפיזם חוץ מהעתקת האפס הוא שיכון כי הגרעין חייב להיות 0). L הוא שדה הפיצול של F לכן $\sigma(L)$ הוא שדה הפיצול של $\sigma(F)$. אבל σ שומר על איברי K שהם המקדמים של F ולכן $\sigma(F) = F$. לפי יחידות $\sigma(L) = L$.
$3 \Rightarrow 4$: ברור. פשוט נצמצם את האוטומורפים על L ואז עפ"י ההנחה.
$4 \Rightarrow 1$ יהי $p \in K[x]$ אי פריק שיש לו שורש $\alpha \in L$ (לכן $K(\alpha) \subseteq L$). יהי $\alpha' \in \tilde{K}$ שורש אחר שלו.
כעת עפ"י משפט יש איזומורפיזם – σ_0 K מ- $K(\alpha)$ ל- $K(\alpha')$ ולכן יש שיכון

$$K(\alpha) \to K(\alpha') \xrightarrow{\text{הכלה}} \tilde{K}$$

לפי מסקנה אפשר להרחיב את σ_0 לאוטומורפיזם $\sigma : \tilde{K} \to \tilde{K}$. לפי הנתון $\sigma(L) = L$ כעת, $\alpha' \in \sigma_0(K(\alpha)) \subseteq \sigma(L)$. □

דוגמא. הרחבה ריבועית היא נורמלית (זה כבר ראינו שיעור קודם).

דוגמא. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ אינה נורמלית. $\sqrt[4]{2}$ שורש של x^4-2 שהינו אי פריק מעל $\mathbb{Q}$ עפ"י קריטריון איזנשטיין. אבל ל- p יש שורשים $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$ ו- $\pm i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$ כי $\pm i\sqrt[4]{2} \notin \mathbb{R}$ ואילו $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$.
$\mathbb{Q}(\sqrt[4]{2}, i)$ היא הרחבה נורמלית של $\mathbb{Q}$. לא קשה לראות שלמעשה

$$\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2})$$

וזה בדיוק שדה שנוצר ע"י כל השורשים של פולינום ולכן עפ"י המשפט.

משפט. יהיו $K \subseteq L$, $F \subseteq M$ אז:

1. אם M/K נורמלית אז M/L נורמלית.
2. אם M/K נורמלית אז LF/F נורמלית.
3. נניח M/K הרחבה אלגברית. אם L/K, K/K נורמליות אז LF/K נורמלית וכן $L \cap K/K$ נורמלית.

הוכחה.

1. יש משפחה $F \subseteq K[x]$ כך ש- M שדה הפיצול של F מעל K. אז M שדה פיצול של F מעל K.
2. יש $F \subseteq K[x]$ כך ש- L שדה הפיצול של F מעל K. אז ניקח את המשפחה הזאת מעל F אז ברור שמקבל השדה הקטן ביותר שמכיל את כל השורשים ואז LF שדה הפיצול של F מעל F.
3. יהי $\tilde{K}$ הסגור האלברי של M. יהי σ אוטומורפזים - K של $\tilde{K}$. שתי ההרחבות הנתונות נורמליות ומוכלות ב- $\tilde{K}$ לכן $\sigma L = L$, $\sigma(F) = F$. צ"ל $\sigma(LF) = LF$, $\sigma(L \cap F) = L \cap F$. אבל σ חח"ע לכן:

$$\sigma(L \cap F) = \sigma(L) \cap \sigma(F) = L \cap F$$

$$\sigma(LF) = \sigma(L)\sigma(F) = LF$$

השוויון $\sigma(LF) = \sigma(L)\sigma(F)$ נובע משתי הכלות. כאשר אגף ימין הוא השדה הקטן ביותר שמכיל $\sigma(L), \sigma(F)$.

□

תרגיל. אם L/K הרחבה אלגברית כלשהי, $\sigma : L \to L$ שיכון- K אז $\sigma(L) = L$.

ריבוי של שורש

נסתכל על K שדה, $\tilde{K}$ סגור אלגברי. יהיו $0 \neq f \in K[x]$ וכן $\alpha \in K$.
קיים $r \geq 0$ שלם יחיד כך שמתקיים:

$$(x-\alpha)^{n+1} \nmid f \qquad (x-\alpha) | f$$

$r \Leftrightarrow r \geq 1$ שורש של f.

הגדרה. α שורש פשוט של f אם $r=1$. α שורש כפול של f אם $r=2$. α שורש מרובה של f אם $r\geq 2$.

הגדרה. יהי $f=\sum_{i=0}^{\infty}a_ix^i\in K[x]$. הנגזרת של f מוגדרת ע"י:

$$f':=\sum_{i=0}^{\infty}i\cdot a_i\cdot x^{i-1}\in K[x]$$

כאשר $i:=\underbrace{1_K+\ldots+1_K}_{i\text{ פעמים}}\in K$.

למה. יהיו $f,g\in K[x]$, $c\in K$.

1. $(f+g)'=f'+g'$.
2. $(cf)'=cf'$.
3. $c'=0$.
4. $(f\cdot g)'=f'\cdot g+g'\cdot f$.
5. $(f\circ g)'=(f'\circ g)\cdot g'$.
כאשר $(f\circ g)(x):=f(g(x))$.

הוכחה. נוכיח רק את 4 כי הכל דומה ורעינו כבר יותר מפעם אחת. עם זאת, 5 הוא תרגיל טוב.
קיימים f_1,f_2 כך ש- $f=f_1+f_2$ ומקיימים $(f_ig)'=f_i'g+f_ig'$ לכל $i=1,2$ (זה לפי הנחת האינדוקציה).

$$\begin{aligned}(f\cdot g)'=((f_1+f_2)\cdot g)'=(f_1g+f_2g)'=(f_1g)'+(f_2g)'=f_1'g+f_1g'+f_2'g+f_2g=\\=(f_1'+f_2')g+(f_1+f_2)g'=f'g+fg'\end{aligned}$$

כעת נותר רק לטפל במקרה הבסיס שהוא המונומים של f והמונומים של g.
בה"כ: $f=\alpha x^n$, $g=\beta x^m$, כאשר $n,m\in\mathbb{N}$, $\alpha,\beta\in K$.

$$\begin{aligned}(fg)'=(\alpha\beta x^{n+m})=(m+n)\alpha\beta x^{n+m-1}=n\alpha\beta x^{n+m-1}+m\alpha\beta x^{n+m-1}=\\=n\alpha x^{n-1}\beta x^m+m\beta x^{m-1}\alpha x^n=f'g+g'f\end{aligned}$$

□

הערה. יהי $f=\sum_{i=0}^{\infty}a_ix^i\in K[x]$. אזי $f'=0\Leftrightarrow ia_i=0\Leftrightarrow a_i=0$ או $i=0$ לכל i $\Leftrightarrow a_i=0$ או $\underbrace{1+\ldots+1}_{i\text{ פעמים}}$ לכל i.
נפריד למקרים:
אם $\operatorname{char}K=0$ אז $f'=0\Leftrightarrow a_i=0$ לכל $i\geq 1\Leftrightarrow f=a_0\in K$.
אם לעומת זאת $\operatorname{char}K=p>0$ (בהכרח p ראשוני) אזי $f'=0\Leftrightarrow a_0=0$ לכל $p\nmid i\Leftrightarrow$ $f=\sum_{i=0}^{\infty}a_{ip}x^{ip}\in K[x]$, $a_{ip}\in K\Leftrightarrow f=g(x^p)$ כאשר $g\in K[x]$, כלומר f הרכבה של פולינום כלשהו על הפולינום x^p.

משפט. יהי $f \in K[x]$ ויהי $\alpha \in L$ שורש של f. אזי f שורש פשוט $\Leftrightarrow$ α לא שורש של f' כלומר $f'(\alpha) \neq 0$.

הוכחה. α שורש של f לכן ניתן לרשום $f = (x-\alpha)g(x)$, $g \in K[x]$.
α שורש פשוט $\Leftrightarrow r = 1 \Leftrightarrow (x-\alpha)^2 \nmid f \Leftrightarrow x - \alpha \nmid g \Leftrightarrow g(\alpha) \neq 0$.
נגזור את f ונקבל:

$$f'(x) = (x-\alpha)g'(x) + g(x)$$

נציב α ונקבל $f'(\alpha) = 0 + g(\alpha)$ כלומר $f'(\alpha) = g(\alpha) \neq 0$.

□

משפט. ל- $0 \neq f \in K[x]$ אין שורשים מרובים ב- $\tilde{K}$ (הסגור האלגברי)(כלומר, כל שורשיו של f הם פשוטים) $\Leftrightarrow gcd(f, f') = 1$

ההוכחה בשיעורי הבית.

דוגמא. נניח $\operatorname{char} K = p > 0$. נסתכל על $f = x^n - 1 \in K[x]$. n זר ל- p. $f' = nx^{n-1}$. קל לראות שאכן $gcd(f, f') = 1$. לכן, אין ל- f שורשים מרובים ב- $\tilde{K}$ כלומר $f = (x-\alpha_1) \cdot \ldots \cdot (x-\alpha_n)$ כאשר $\alpha_1, \ldots, \alpha_n \in \tilde{K}$ שונים זה מזה והם השורשים ה- nים של a.
לעומת זאת, עבור $g(x) = x^p - 1$, $g'(x) = px^{p-1} = 0$ ולכן $\gcd(g, g') = x^p - 1 \neq 1$.
לכן יש שורשים מרובים. ואכן, מתקיים $x^p - 1 = (x-1)^p$ כלומר קיים שורש שהוא 1 מרובה מריבוי p.

משפט. יהי $f \in K[x]$ אי פריק. אזי ל- f יש שורשים מרובים ב- $\tilde{K}$ $\Leftrightarrow f' = 0$.

הוכחה. $\Rightarrow$: אם $f' = 0$ אזי $gcd(f, f') = f \neq 1$ ולכן ל-f יש שורשים מרובים.
$\Leftarrow$: נניח בשלילה $f' \neq 0$. יהי $d \in gcd(f, f')$. $d|f$ ולכן $\deg(d) \leq \deg(f') < \deg f$.
אולם גם $d|f$, d ממעלה קטנה ממש מהמעלה של f ו-f אי פריק, לכן d הפיך ולכן $1 \in \gcd(f, f')$ ואז אין ל- f שורשים מרובים. סתירה. לכן $f = 0$.

□

מסקנה. יהי $f \in K[x]$ אי פריק.

1. אם $\operatorname{char} K = 0$ אז אין ל- f שורשים מרובים.
2. אם $\operatorname{char} K = p > 0$ אז ל- f יש שורשים מרובים $\Leftrightarrow f(x) = g(x^p)$.

וזה בגלל המשפט האחרון והדוגמא הקודמת.

דוגמא. נבחר $k = \mathbb{F}_p(t)$ שדה הפונקציות הרציונליות מעל $\mathbb{F}_p$. (כאשר $\mathbb{F}_p(t)$ הוא שדה התמונות של $\mathbb{F}_p[t]$).
$f(x) = x^p - t \in K[x]$ הוא א"פ (לפי קריטריון איזנשטיין עם הראשוני t). לכן מהמסקנה יש ל- f שורשים מרובים. אם $\alpha \in K$ שורש אז $\alpha^p = t$ ואז $f = x^p - t(x-\alpha)^t$.