

אלגברה ב' 2 – תרגול 5

28.03.11

שדה פיצול

הגדרה. $L \supset K$ הוא שדה פיצול של $F \subseteq K[x]$ מעל K אם לכל $f \in F, f \neq 0$, מתפצל לחלוטין ב- L ו- L נוצר מעל K ע"י שורשי פולינומים ב- F .

שאלה. יהי $f \in K[x]$ ממעלה n . אז $[L : K] \leq n!$ כאשר L שדה הפיצול של f מעל K .

תשובה. באינדוקציה על n . ל- $n = 1$, $f = ax + b, a, b \in K$ עבור $L = K(\frac{b}{a}) = K$ והטענה אמת.

נניח עד $n - 1$ ונוכיח ל- n .

יהי $p \in K[x]$ א"פ כך ש- $p|f$ (מניחים בפרט $n > 1$). יהי $\alpha \in L$ שורש של p . מדוע יש כזה? כי L שדה הפיצול של f . אז $(x - \alpha)|f$ מעל L , נכתוב $f(x - \alpha)g$ עבור $g \in L[x]$. מכיוון ש- $(x - \alpha) \in K[\alpha][x]$, $f, (x - \alpha) \in K[\alpha][x]$ מתקיים גם $(x - \alpha)|f$ מעל $K[\alpha]$ (באופן כללי, אם $f_2 = qf_1 + r$ נכתוב $f_1|f_2$ ב- F' אז $f_1|f_2$ ב- F). נכתוב $f_2 = qf_1 + r$ עבור $f_1, f_2 \in F[x]$ ועבור $F' \subseteq F$ ו- $f_1|f_2$ ב- F' אז $f_1|f_2$ ב- F . $r = 0, q, r \in F[x]$ ומיחידות $q, r \in F[x]$.

לכן $g \in K[\alpha][x]$ אז L הוא שדה פיצול של g מעל $K[\alpha]$, $K[\alpha]$ מתפצל ב- L כי f מתפצל ב- L , L נוצר מעל $K[\alpha]$ ע"י שורשי g . מאינדוקציה $[L : K[\alpha]] \leq (n - 1)!$ כעת,

$$[L : K] = \underbrace{[L : K[\alpha]]}_{\leq (n-1)!} \underbrace{[K[\alpha] : K]}_{\leq \deg p \leq n}$$

שאלה. יהי p ראשוני. $\mathbb{Q}[x] \ni f = x^{p-1} + x^{p-2} + \dots + x + 1$. מצאו את שדה הפיצול $\mathbb{C} \supset L$ של f מעל $\mathbb{Q}$.

תשובה. מעל $\mathbb{Q}(x), f = \frac{x^p - 1}{x - 1}$. הראינו בתרגול קודם ש- f א"פ מעל $\mathbb{Q}$. שורשי f הם השורשים של $x^p - 1$ פרט ל- 1 . נבחר $\xi \in \mathbb{C}$ כך ש- $\xi^p = 1$ ואז $\xi, \xi^2, \dots, \xi^{p-1}$ הם שורשים שונים. לכן $\mathbb{Q}[\xi]$ הוא שדה הפיצול של f מעל $\mathbb{Q}$. $[\mathbb{Q}[\xi] : \mathbb{Q}] = p - 1$

שאלה. תארו את שדה הפיצול של $x^4 - x^2 + 4$ מעל $\mathbb{Q}$ (חלקי ל- $\mathbb{C}$) ומצאו את מעלתו מעל $\mathbb{Q}$.

תשובה.

$$x^4 - x^2 + 4 = 0 \Rightarrow x^2 = \frac{1 \pm \sqrt{15}i}{2}$$

נכתוב $x = u + iv$ עבור $u, v \in \mathbb{R}$.

$$(u + iv)^2 = \frac{1 \pm \sqrt{15}i}{2}$$

נשווה חלק ממשי ומדומה:

$$u^2 - v^2 = \frac{1}{2}$$

$$2uv = \pm \frac{\sqrt{15}}{2}$$

לכן,

$$v = \pm \frac{\sqrt{15}}{4u}$$

נציב בחזרה:

$$u^2 - \frac{15}{16u^2} = \frac{1}{2}$$

$$16u^4 - 8u^2 - 15 = 0$$

רק שעכשיו יודעים שיש פתרון בממשיים.

$$u^2 = \frac{8 \pm \sqrt{64 + 64 \cdot 15}}{32} = \frac{1 \pm 4}{4} \quad \text{כי } u^2 > 0 \quad \frac{5}{4}$$

אז

$$u = \pm \frac{\sqrt{5}}{2} \quad v = \pm \frac{\sqrt{3}}{2}$$

לכן,

$$x = \pm \frac{\sqrt{5} \pm i\sqrt{3}}{2}$$

$$x^4 - x^2 + 4 =$$

$$\begin{aligned} &= \left(x - \frac{\sqrt{5} + i\sqrt{3}}{2}\right) \left(x - \frac{\sqrt{5} - i\sqrt{3}}{2}\right) \left(x + \frac{\sqrt{5} + i\sqrt{3}}{2}\right) \left(x + \frac{\sqrt{5} - i\sqrt{3}}{2}\right) = \\ &= (x^2 - \sqrt{5}x + 2)(x^2 + \sqrt{5}x + 2) \end{aligned}$$

זה פירוק למכפלת א"פ מעל $\mathbb{R}$. שדה הפיצול הוא

$$\mathbb{Q}[\sqrt{5} + i\sqrt{3}, \sqrt{5} - i\sqrt{3}] = \mathbb{Q}[\sqrt{5} + i\sqrt{3}, \sqrt{5}]$$

אפשר היה כמובן לרשום פשוט את כל השורשים, אבל כדי שיהיה נוח לעבוד עם השדה נרצה למצוא כמה שפחות שורשים.

נמצא את מעלת שדה הפיצול. $\sqrt{5} + i\sqrt{3}$ אלגברי- $\mathbb{Q}$ ממעלה 4 כי $x^4 - x^2 + 4$ א"פ - $\mathbb{Q}$ (מצד אחד השורשים שלו לא ב- $\mathbb{Q}$ עדיין צריך להסביר מדוע הוא לא מכפלת א"פ ממעלה 2, וזה כי מצאנו ככתיבה כמכפלת א"פ מעל $\mathbb{R}$ ומיחידות הפירוק היינו מקבלים $\sqrt{3}, \sqrt{5}$ ב- $\mathbb{Q}$).

נראה ש- $\sqrt{5} \in \mathbb{Q}[\sqrt{5} + i\sqrt{3}]$. נסמן $\gamma = \frac{\sqrt{5} + i\sqrt{3}}{2}$ אז $c = \gamma^2 - \sqrt{5}\gamma + 2 = 0$

$$\sqrt{5}\gamma = \gamma^2 + 2 \in \mathbb{Q}[\gamma] \Rightarrow_{\mathbb{Q}[\gamma] = \mathbb{Q}(\gamma)} \sqrt{5} \in \mathbb{Q}[\gamma]$$

שאלה. יהיו $F \subset K, E \subset L$ שדות. נניח כי K/F אלגברי. הוכיחו כי $F[K \cup E]$ הוא שדה וכי $F[K \cup E]/E$ אלגברית.

תשובה.

$$F[K \cup E] = E[K]$$

איברי K אלגבריים מעל F ולכן גם מעל E . נוכיח ש- $E[K] = E(K)$. כל $u \in E[K]$ הוא מהצורה $u = \sum_{i=1}^n e_i k_i, k_i \in K, e_i \in E$. אז u אלגברי מעל K , $E(k_1, \dots, k_n) = E$ אלגבריים- k_i . אם $u^{-1} \in E(k_1, \dots, k_n) = E(k_1, \dots, k_n), u \neq 0$. לכן $E[K]/E$ שדה, $E[K]$ שדה.