31.10.13 בס״ד כ״ז חשוון תשע״ד

אלגברה מופשטת 3 - הרצאה מס' 3.

יהי $f\in F[x]$

שדה $F\le K$ נקרא <u>שדה מפצל</u> של F אם ב-$K[x]$ אפשר לכתוב $f(x)=(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$, כלומר $\alpha_1,\dots,\alpha_n\in K$.

<u>משפט:</u> לכל פולינום ממעלה n מעל שדה F יש שדה מפצל $F\le K$ כך ש- $[K:F]\le n!$.

<u>הוכחה:</u> באינדוקציה על n.

אם f פריק, $\underset{n=m+k}{f=g\cdot h}$ ואז, יש שדה מפצל $F\le K$ ל-g כך ש $[K:F]\le m!$.

יש שדה מפצל $K\le E$ ל-h כך ש $[E:K]\le k!$

$$[E:F]=[E:K]\cdot[K:F]\le m!\,k!=\frac{n!}{\binom{n}{m}}\le n!$$

אחרת, f אי-פריק ואז ניקח $F\le F_1=F[x]/\langle f\rangle$

ושם (ב-F_1) יש שורש $\alpha\in F_1$ (*) ל-f, כלומר ניתן לכתוב $f(x)=(x-\alpha)\cdot \underset{\deg(g)=n-1}{g(x)}$

לפי הנחת האינדוקציה, יש שדה מפצל $F_1\le K$ של g, כך ש $[K:F_1]\le(n-1)!$. ואז, $[K:F]=[K:F_1]\cdot[F_1:F]\le(n-1)!\cdot n=n!$.

(*) <u>הערה:</u> יהי F שדה עם פולינום אי-פריק $f\in F[x]$.

ניקח $F_1=F[x]/\langle f\rangle$, שדה.

נראה שב-F_1 יש שורש ל-f:

נסמן $\alpha=x+\langle f\rangle$.

נכתוב $f(x)=\sum a_ix^i$ כאשר $a_i\in F$.

נבדוק: $f(\alpha)=\sum a_i\alpha^i=\sum a_i(x+\langle f\rangle)^i=$

$=\sum a_i(x^i+\langle f\rangle)=\sum(a_ix^i+\langle f\rangle)=$

$=(\sum a_ix^i)+\langle f\rangle=f(x)+\langle f\rangle=\langle f\rangle$

<u>דוגמה:</u> $F_1=\mathbb{Q}[\rho_3]=\mathbb{Q}[\sqrt{-3}]$, $f(x)=x^3-2$

ρ, $\rho^3=1$

$\boxed{\rho_n=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}\qquad \rho_3=\frac{-1+\sqrt{-3}}{2}}$

<u>כנ"ל</u>

מחפשים הרחבה של F_1 שמפצלת את f.

(יודעים ש- f אי-פריק מעל F_1)

לוקחים $F_2 = F_1[\lambda]/\langle\lambda^3-2\rangle$

נסמן $\alpha = \lambda + \langle\ \rangle$

$\alpha^3 = 2$

בנוסף, גם $(\rho\alpha)^3 = 2$, $(\rho^2\alpha)^3 = 2$.

ואז, $(\lambda-\alpha)(\lambda-\rho\alpha)(\lambda-\rho^2\alpha) = \lambda^3-(\alpha+\rho\alpha+\rho^2\alpha)\lambda^2 +$
$+(\rho+\rho^2+1)\alpha^2\lambda - \alpha\cdot\rho\alpha\cdot\rho^2\alpha = \lambda^3-\alpha^3 = \lambda^3-2$

$$\begin{array}{c} F_2 \\ | \\ F_1 = \mathbb{Q}[\rho] \\ | \\ \mathbb{Q} \end{array}$$

<u>דוגמה 2:</u> הפעם נבנה שדה מפצל מעל $\mathbb{Q}$. (לאותו פולינום)

אפשר לבנות $K_1 = \mathbb{Q}[\lambda]/\langle\lambda^3-2\rangle$
$= \{a+\beta\lambda+\gamma\lambda^2+\langle\ \rangle \mid a,\beta,\gamma\in\mathbb{Q}\}$

$\alpha = \lambda + \langle\lambda^3-2\rangle$

חולק (עם שארית): $\mu^3-2 = (\mu-\alpha)\underbrace{(\mu^2+\alpha\mu+\alpha^2)}_{g(x)}$

מהם השורשים של $g(x)$?

$$\frac{-\alpha\pm\sqrt{\alpha^2-4\alpha^2}}{2} = \alpha\cdot\frac{-1\pm\sqrt{-3}}{2} \notin K_1$$

כעת בונים $K_2 = K_1[\mu]/\langle\mu^2+\alpha\mu+\alpha^2\rangle =$
$= \mathbb{Q}[\lambda,\mu]/\langle\lambda^3-2,\ \mu^2+\lambda\mu+\lambda^2\rangle$

$$\begin{array}{rc} & K_2 \\ & | \\ 1+2 & K_1 \\ & | \\ 3 & \mathbb{Q} \end{array}$$

<u>גישה אחרת:</u>

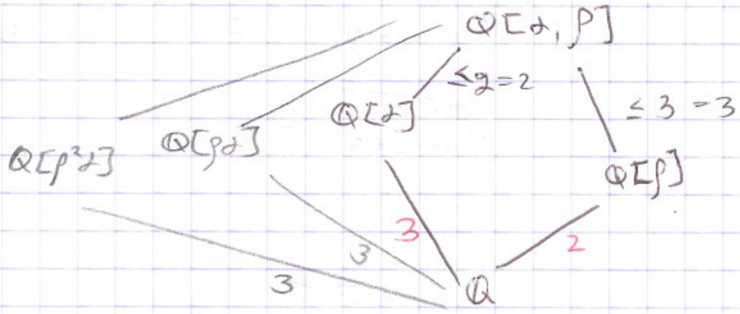
<u>משפט:</u> לכל שדה F יש "סגור אלגברי", שהוא שדה $\bar{F}$ שהוא אלגברי מעל F, ויש בו שורש לכל פולינום עם מקדמים ממנו ($\bar{F}$).

איבר אלגברי: מאפס פולינום בעל מקדמים מ- F.

<u>דוגמה:</u> $\mathbb{C}$ סגור אלגברית.

כעת, מחפשים ב- $\mathbb{C}$ שורשים ל- x^3-2: $\alpha = \sqrt[3]{2}$, $\rho\alpha$, $\rho^2\alpha$.

לכן $\mathbb{Q}[\alpha,\rho\alpha,\rho^2\alpha] = \mathbb{Q}[\alpha,\rho]$ מפצל את x^3-2



עפ"י משפט $[\mathbb{Q}[\alpha,\rho]:\mathbb{Q}[\rho]]\le 3$, $[\mathbb{Q}[\alpha,\rho]:\mathbb{Q}[\alpha]]\le 2$

אבל $(3,2)=1$ לכן בהכרח $[\mathbb{Q}[\alpha,\rho]:\mathbb{Q}[\rho]]=3$,

$[\mathbb{Q}[\alpha,\rho]:\mathbb{Q}[\alpha]]=2$.

<u>משפט כללי</u>: נניח ש- $f\in\mathbb{Q}[x]$, והשורשים שלו ב- $\mathbb{C}$ הם $\alpha_1,\dots,\alpha_n$

אז $\mathbb{Q}[\alpha_1,\dots,\alpha_n]$ מפצל את הפולינום והמימד שלו $\le n!$.

<u>תרגיל</u>: מדוע המימד $\le n!$?

<u>הגדרה</u>: $f\in F[x]$.

<u>שדה פיצול</u> של f מעל F הוא שדה מפצל מינימלי (= אין לו תת-שדות מפצלים).

<u>דוגמה</u>: $\mathbb{Q}[\alpha_1,\dots,\alpha_n]$ הוא שדה פיצול של הפולינום ששורשיו $\alpha_1,\dots,\alpha_n$

<u>הוכחה שתמיד קיים שדה פיצול</u>: נבנה שדה מפצל <u>ממימד סופי</u>,

תת-שדה מפצל מינימלי הוא שדה פיצול.

שיכון של שדות: הומו' $F\to E$ (חח"ע)

כמובן הכלה של תת-שדה בשדה האם היא שיכון.

<u>דוגמה</u>: $\mathbb{Q}[\sqrt{-1}]\hookrightarrow\mathbb{C}$ בשתי דרכים: $\sqrt{-1}\to i$, $\sqrt{-1}\to -i$

תזכורת: תת השדה הראשוני של F = $\underbrace{\text{השדה הנוצר ע"י } 1}$ = $\mathbb{F}_p$, $\mathbb{Q}$. $\left\{\pm\frac{1+\dots+1}{1+\dots+1}\right\}$

לשדה ראשוני יש לכל היותר שיכון אחד בשדה F.

<u>המשכה של שיכון</u>: יש שיכון $F\overset{\phi}{\hookrightarrow}E$ ו- $F\subseteq F_1$.

שיכון $F_1\overset{\phi_1}{\hookrightarrow}E$ מהווה המשכה של ϕ אם

$\phi_1|_F=\phi$.

$$\begin{tikzcd} F_1 \arrow[dr, dashed] & \\ F \arrow[u, phantom, "\cup"] \arrow[r, hook] & E \end{tikzcd}$$

<u>סימון</u>: $n^{F_1}_{F\hookrightarrow E}$ = מספר ההמשכות של $F\hookrightarrow E$ ל- F_1 .

דוגמאות: $n^{\mathbb{Q}[\sqrt{-7}]}_{\mathbb{Q}\hookrightarrow\mathbb{C}} = 2$

$n^{\mathbb{Q}[\sqrt{-7}]}_{\mathbb{Q}\hookrightarrow\mathbb{R}} = 0$

עוד דוגמאות: $n^{\mathbb{Q}[\sqrt{2},\sqrt{3}]}_{\mathbb{Q}\hookrightarrow\mathbb{R}} = 4$

$n^{\mathbb{Q}[\sqrt{2},\sqrt{3}]}_{\mathbb{Q}[\sqrt{2}]\hookrightarrow\mathbb{R}} = 2$

<u>למה:</u> $F_1=F[a]$, נניח f הוא הפולינום המינימלי של a, מעל F.

ונניח $\phi: F \longrightarrow E$ שיכון. אז $\boxed{n^{F_1}_{F\hookrightarrow E} = \text{מס' השורשים של } \phi(f) \text{ מעל } E}$

<u>הוכחה:</u> לכל המשכה $F_1 \xrightarrow{\phi'} E$

ניקח את הפולינום $\phi(f)$ ונציב בתוכו את המספר $\phi'(a)$:

$$(\phi(f))(\phi'(a)) = (\phi'(f))(\phi'(a)) = \phi'(f(a)) =$$
$$= \phi'(0) = 0$$

קיבלנו $\phi'(a)$ שורש של $\phi(f)$, וכל בחירה שההמשכה

נקבעת ע"י התמונה של a.

הכיוון $\le$.

הכיוון ההפוך, יהי $\beta\in E$ שורש של $\phi(f)$,

נראה שיש המשכה המקיימת $a\longmapsto\beta$.

$F_1 \cong F[x]/\langle f\rangle$,

נגדיר הומו' $F[x]\longrightarrow E$ לפי $x\longmapsto\beta$; הגרעין הוא $\langle f\rangle$.

לכן איזו' I יש הומו'

$$F_1 \cong F[x]/\langle f\rangle \longrightarrow E$$
$$a \longmapsto x+\langle f\rangle \longrightarrow \beta$$

<u>מסקנות:</u>

1. $\underbrace{n^{F_1}_{F\hookrightarrow E}}_{\text{מספר השורשים ב-}E} \le [F_1:F] = \deg f$

2. יש המשכה $\Longleftrightarrow$ יש לפחות שורש אחד ב-E.

<u>הגדרה:</u> $g\in E[x]$ מתפצל. g <u>ספרבילי</u> אם יש לו בדיוק $\deg g$ שורשים שונים.

31.10.13 כ"ז חשוון תשע"ד בס"ד

<u>משפט</u>: יהי $\phi: F \hookrightarrow E$ שיכון.

1. לכל הרחבה סופית K של F,

$$n^{K}_{F\hookrightarrow E} \le [K:F]$$

2. נניח ש- K נוצר מעל F ע"י השורשים של פולינום f, כך ש- $\phi(f)$ מתפצל ב- E. אזי:

(א) יש המשכה של ϕ ל- $K \hookrightarrow E$.

(ב) אם $\phi(f)$ ספרבילי אז: $n^{K}_{F\hookrightarrow E} = [K:F]$.

$$\begin{array}{ccc} K & & \\ | & & \\ F_1 & & \\ | & & \\ F & \longrightarrow & E \end{array}$$

<u>הוכחה</u>: 1. נכתוב $K = F[a_1, \dots, a_t]$

נסמן: $F_1 = F[a_1]$. לפי הלמה יש $n^{F_1}_{F\hookrightarrow E} \le [F_1:F]$

המשכות של ϕ אל F_1. באינדוקציה על t, לכל אחת מהן

$n^{K}_{F_1 \xrightarrow[\phi']{} E} \le [K:F_1]$. לכן,

$$n^{K}_{F\hookrightarrow E} = \sum_{\phi'} n^{K}_{F_1\hookrightarrow E} \le [K:F_1]\cdot[F_1:F] = [K:F]$$

$F[a]$

2. אפשר להניח ש- $a_1, \dots, a_n$ הם השורשים של f,

כאשר $\phi(f)$ מתפצל ב- E. כמקודם נסמן $F_1 = F[a_1]$.

(א) נסמן ב- f_1 את הפולי' המינימלי של a_1 מעל F.

כמובן $f_1 | f$.

הנחנו ש- $\phi(f)$ מתפצל ב- E ולכן $\phi(f_1)$ מתפצל ב- E.

לכן לפי הלמה $n^{F_1}_{F\hookrightarrow E} =$ מספר השורשים של $\phi(f_1)$ ב-E ≥ 1

נסמן המשכה כזו ב- $\phi_1: F_1 \longrightarrow E$.

תנאי המשפט חלים על K/F_1 ולכן הנחת האינדוקציה

$$1 \le n^{K}_{\phi_1: F_1 \to E} \le n^{K}_{F\to E}$$

(ב) כאשר $\phi(f)$ ספרבילי, גם $\phi(f_1)$ ספרבילי,

אז

$$n^{K}_{F\to E} = \sum_{\substack{\phi_1: F_1 \to K \\ \text{המשכה}}} n^{K}_{F_1 \xrightarrow{\phi_1} E} = [K:F_1]\cdot[F_1:F] = [K:F]$$

משפט: שדה הפיצול של f מעל F הוא יחיד עד כדי איזומורפיזם.

הוכחה: יהיו K, K' שדות פיצול.

K נוצר מעל F ע"י השורשים של f.

אבל f מתפצל ב- K'.

לכן יש שיכון $K \hookrightarrow K'$.

התמונה של K מפצלת, אבל K' מינימלי ולכן שווה לתמונה הנ"ל. כלומר $K \cong K'$.

הגדרה: נסמן את שדה הפיצול של הפולינום x^2+1

מעל $\mathbb{Q}$: $\mathbb{Q}[\sqrt{-1}]$

$\mathbb{R}$: $\mathbb{C}$

$\mathbb{C}$: $\mathbb{C}$

$\mathbb{Q}[\sqrt{2}]$: $\mathbb{Q}[\sqrt{2}, \sqrt{-1}]$

$\quad = $

$\mathbb{Q}[\sqrt{-2}]$: $\mathbb{Q}[\sqrt{-2}, \sqrt{-1}]$