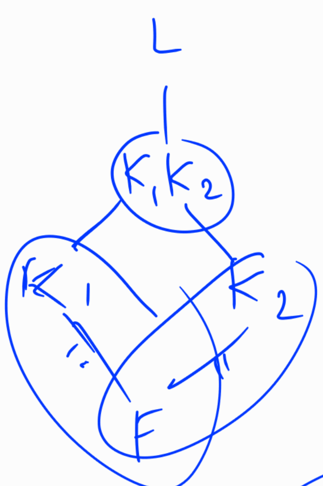
תורת גלואה — תרגול 3

תזכורת: כפליות המגדל? $F\subseteq K\subseteq L$

$$[L:F]=[L:K]\cdot[K:F]$$

<u>תרגיל</u>: תהי L/F הרחבה סופית ויהיו K_1,K_2 שדות ביניים כך ש- $[K_1:F],[K_2:F]$ זרים.

הוכח: $[K_1K_2:F]=[K_1:F][K_2:F]$.



<u>פתרון</u>: ברור: $[K_i:F]\mid[K_1K_2:F]$ $\forall i=1,2$

מכיוון שהם זרים: $\overbrace{[K_1:F]}^{m_1}\overbrace{[K_2:F]}^{m_2}\mid[K_1K_2:F]$.

צריך שוויון. יהי $\{b_1,\dots,b_{m_1}\}$ בסיס ל- K_1/F, $\{c_1,\dots,c_{m_2}\}$ בסיס ל- K_2/F.

ולכן $K_1K_2=\mathrm{Span}_F\{b_ic_j\}_{i=1,j=1}^{m_1,m_2}$ כי

$$[K_1K_2:F] \le m_1m_2$$

לכן $[K_1K_2:F] = [K_1:F][K_2:F]$. מ.ש.ל.

תרגיל: תהי K/F הרחבה סופית ויהי $p(x)\in F[x]$ אי-פריק. $\deg p \nmid [K:F]$.

אז ל-p אין שורש ב-K.

פתרון: נניח בשלילה כי יש שורש $p(\alpha)=0$, $\alpha \in K$.

$$\begin{array}{c} K \\ | \\ F(\alpha) \\ | \\ F \end{array}$$

p אי"פ $\Leftarrow$

$[F(\alpha):F] = \deg p$

$\uparrow$

$\left(\dfrac{F[x]}{\langle p(x) \rangle} \cong F(\alpha) \right)$

ולכן מכפליות המעלות נקבל:

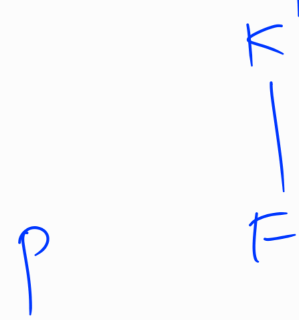
$$\deg p = [F(\alpha):F] \mid [K:F]$$

בסתירה לנתון.

מ.ש.ל.

מסקנה: למשל, $\sqrt[21]{6} \notin \mathbb{Q}(\sqrt[9]{10})$.

הערה: ההרחבה הקודם לא אומר ש-p נשאר אי-פריק מעל K.



למשל $K=\mathbb{Q}(\sqrt[6]{2})/\mathbb{Q}$, $p(x)=x^4-2$.

$p(x)=(x^2-\sqrt{2})(x^2+\sqrt{2}) \Leftarrow \sqrt{2}\in K$

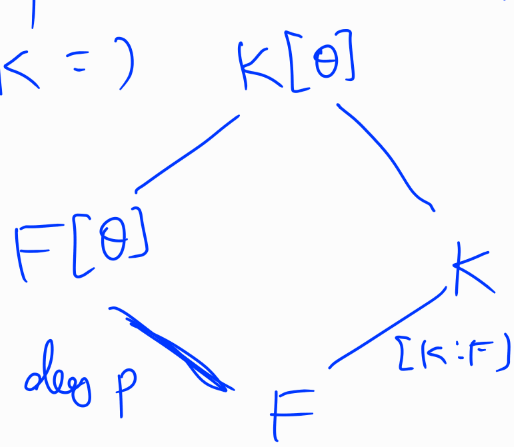
מעל K.

תרגיל: תהי K/F הרחבה סופית, $p\in F[x]$ אי"פ, כך ש-$[K:F]$, $\deg p$ זרים.

אז $p(x)$ נשאר אי-פריק מעל K.

הוכחה:

$(F[\theta]\cdot K=)$



$$\frac{F[x]}{\langle p(x)\rangle} \cong F[\theta]$$

מהתרגיל הראשון היום אנו יודעים כי

$$[K[\theta]:F] = [K:F]\cdot \deg p$$

$$\| $$

$$[K[\theta]:K]\cdot[K:F]$$

נקבל כי: $[K[\theta]:K] = \deg p$.

מסקנה: p אי-פריק מעל K.

הסבר:

$$\underbrace{\frac{K[x]}{\langle p(x)\rangle}}_{\deg p} \xrightarrow{x \mapsto \theta} \underbrace{K[\theta]}_{[K[\theta]:K]=\deg p}$$

לכן ההעתקה הזו היא $\cong$, לפי

לכן $p(x)$ אי-פריק מעל K). שכן $\frac{K[x]}{\langle p(x)\rangle}$ שדה.

מ.ש.ל.

פיצול פולינומים

תזכורת מההרצאה –

פולינום מתפצל מעל שדה = שווה למכפלת פולינומים לינאריים מעל אותו שדה.

שדה פיצול = שדה מינימלי שמעליו הפולינום מתפצל = השדה הנוצר ע"י סיפוח כל שורשי הפולינום.

תרגיל: חשבו שדה פיצול של $f(x)=x^3-2$.
מה ממדו? [מעל $\mathbb{Q}$.]

פתרון: מהם שורשיו המרוכבים של f?

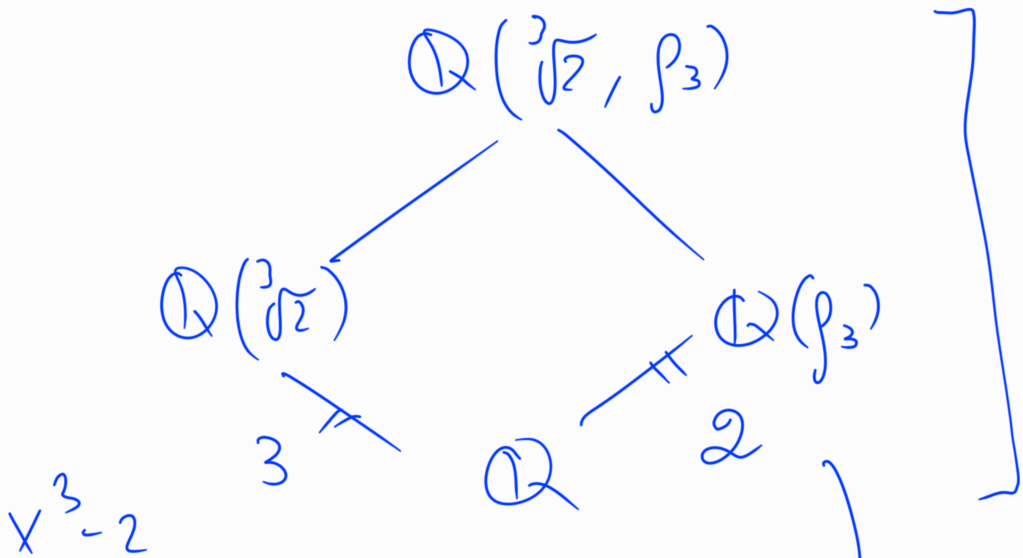
$$\sqrt[3]{2}\ ,\quad \rho_3\sqrt[3]{2}\ ,\quad \rho_3^2\sqrt[3]{2}$$

כאשר: $\rho_3=e^{\frac{2\pi i}{3}}$. (סימון: $\rho_n=e^{\frac{2\pi i}{n}}$.)

$$\mathbb{Q}_f=\mathbb{Q}\left(\sqrt[3]{2},\ \rho_3\sqrt[3]{2},\ \rho_3^2\sqrt[3]{2}\right)=$$

$$=\mathbb{Q}\left(\sqrt[3]{2},\ \rho_3\sqrt[3]{2}\right)=$$

$$=\mathbb{Q}\left(\sqrt[3]{2},\ \rho_3\right)$$



$$\rho_3^3 = 1$$

$$\Downarrow$$

$$\cancel{(\rho_3 - 1)}\underbrace{(\rho_3^2 + \rho_3 + 1)}_{=\,0} = 0$$

[פ' אוילר: נגלה כי: $\varphi(n) = [\mathbb{Q}(\rho_n) : \mathbb{Q}]$.]

$$\rho_n = e^{\frac{2\pi i}{n}}$$

2, 3 זרים $\Leftarrow$ $.[\underbrace{\mathbb{Q}(\sqrt[3]{2}, \rho_3)}_{\mathbb{Q}_f} : \mathbb{Q}] = 6$

ש.פ.ל.

תרגיל: יהי p ראשוני ויהי $\alpha \in \mathbb{F}_p^\times$.

נתבונן ב- $f(x)=x^p - x + \alpha$.

נמצא את שדה הפיצול של f.

פתרון: נזכיר כי לכל $\beta \in \mathbb{F}_p$ מתקיים

$$\beta^p = \beta$$

ולכן $f(\beta) = \alpha \neq 0$, כלומר ל-f אין שורשים מעל $\mathbb{F}_p$.

יתרה מזאת, $f(x)$ אי-פריק מעל $\mathbb{F}_p$.

יהי θ שורש של $f(x)$. אזי:

$$f(\theta+1) = (\theta+1)^p - (\theta+1) + \alpha =$$

$$= \theta^p - \theta + \alpha = 0$$

כי מעל $\mathbb{F}_p$, $(x+y)^p = x^p + y^p$.

בדומה:

$$f(\theta+2) = \dots = f(\theta+(p-1)) = 0$$

כלומר, שדה הפיצול של f: $\mathbb{F}_p(\theta)$ כי כל השורשים שייכים לשדה זה.

ולכן ממדו: p.

נניח בשלילה כי f פריק: (מעל $\mathbb{F}_p$)

$$f = g_1 \cdot g_2$$

כאשר

$$g_1 = \prod_{i\in S}\left(x-(\theta+i)\right)$$

כאשר $\emptyset \neq S \subsetneq \mathbb{F}_p$.

כעת נפתח את g_1 ונחשב את המקדם של $x^{|S|-1}$:

$$a_{|S|-1} = -\sum_{i\in S}\theta+i =$$

$$= -|S|\cdot\theta - \sum_{i\in S} i$$

לכן: $a_{|S|-1}\in\mathbb{F}_p$, $\sum_{i\in S} i \in \mathbb{F}_p$

ולכן: $\underbrace{-|S|}_{\neq 0}\cdot\theta\in\mathbb{F}_p \Rightarrow \theta\in\mathbb{F}_p$,

בסתירה.

מש"ל.