תזכורת

משפט: יהיו $F\subset K\subset E$ שדות. אזי $[E:F]=[E:K][K:F]$

תרגיל

אם $a,b\in E\backslash F$ כך ש $\begin{matrix}[F(a):F]=m\\ [F(b):F]=n\end{matrix}$, אזי $(m,n)=1$ גורר $[F(a,b):F]=m\cdot n$.

פתרון

$$\begin{tikzcd}[column sep=small] & F(a,b) \arrow[dl, dash] \arrow[dr, dash] & \\ F(a) \arrow[dr, dash, "m"'] & & F(b) \arrow[dl, dash, "n"] \\ & F & \end{tikzcd}$$

$$[F(a,b):F]=[F(a,b):F(a)][F(a):F]=m\cdot[F(a,b):F(a)]=$$

$$=[F(a,b):F(b)]\cdot[F(b):F]=n\cdot[F(a,b):F(b)]$$

לכן $n,m\mid[F(a,b):F]$, ומכיוון שm,n זרים $\Longleftarrow$ $mn\mid[F(a,b):F]$.

$[F(b):F]=n$ ולכן קיים פולינום מינימלי לb מעל F שהוא מדרגה n. נסמן אותו בg_b. $g_b(b)=0$.

הפולינום $g_b\in F[x]$ $\Longleftarrow$ $g_b\in F(a)[x]$, ולכן דרגת הפולינום המינימלי של b מעל $F[a]$ היא לכל היותר n.

לכן $[F(a,b):F(a)]\le n$ ($F(a,b)=F(a)(b)$) $\Longleftarrow$ $[F[a,b]:F]\le m\cdot n$ $\Longleftarrow$ $[F(a,b):F]=mn$

תרגיל

$f(x),g(x)\in F[x]$ פולינומים אי־פריקים כך ש$\deg f=6,\deg g=5$. נתון $a\in E\backslash F$ שהוא שורש של f. הוכיחו או הפריכו: $g(x)$ אי־פריק מעל $F(a)$.

פתרון

ניתן להניח ש־E יש שורש של $g\left(x\right)$: $b\in E$ כך ש־$g\left(b\right)=0$.

$$\begin{tikzcd}
 & F\left(a,b\right) \arrow[dl, dash, "5"'] \arrow[dr, dash, "6"] & \\
F\left(a\right) \arrow[dr, dash, "6"'] & & F\left(b\right) \arrow[dl, dash, "5"] \\
 & F &
\end{tikzcd}$$

לפי התרשים והתרגיל הקודם הפולינום המינימלי של b מעל $F\left(a\right)$ הוא מדרגה 5. אבל $g\left(x\right)$ הוא פולינום כזה ולכן הוא אי־פריק.

תרגיל

$u\in E\backslash F$ עם פולינום מינימלי $m_{u}\left(x\right)=x^{n}-a$ מעל F.
יהי $m\in\mathbb{N}$. מצאו את הפולינום המינימלי של u^{m}(נסמן $m_{u^{m}}\left(x\right)$).

פתרון

שלב א: נניח ש־$n\mid m$.

$$0=m_{u}\left(u\right)=u^{n}-a=\left(u^{m}\right)^{n/m}-a$$

$f\left(x\right)=x^{n/m}-a$ שמאפס את u^{m} $\Longleftarrow$ $\deg m_{u^{m}}\leq\frac{n}{m}$.
נניח ש־$g\left(x\right)=x^{t}+\cdots$, $t<\frac{n}{m}$ מאפס את u^{m}. אזי

$$0=g\left(u^{m}\right)=u^{mt}+\cdots$$

$mt<n$ בסתירה למינימליות m_{u}.

$$\Longrightarrow\ \deg m_{u^{m}}=\frac{m}{n}$$

$$m_{u^{m}}=x^{n/m}-a$$

שלב ב: m כללי.

$$d=\left(m,n\right)\qquad d\mid n$$

$$m_{u^{d}}=x^{\frac{n}{d}}-a$$

$$m_{u^{d}}\left(u^{m}\right)=u^{\frac{mn}{d}-a}=\left(u^{n}\right)^{m/d}-a=a^{m/d}-a$$

$$f(x) = x^{n/d} - a^{m/d}$$

$$f(u^m) = 0$$

$$\deg m_{u^m} \leq \frac{n}{d}$$

קיימים $s,t \in \mathbb{Z}$ כך ש$d = ms + nt$.

$$F(u^m) = F\left(u^d\right)$$

$$u^m = \left(u^d\right)^{m/d} \in F\left[u^d\right]$$

$$\implies F(u^m) \subseteq F\left(u^d\right)$$

$$u^d = u^{ms+nt} = \underbrace{u^{ms}}_{\in F(u^m)} \cdot \underbrace{u^{nt}}_{a^t \in F} \in F(u^m)$$

$$\implies F\left(u^b\right) \subseteq F(u^m)$$

$$\implies F\left(u^b\right) = F(u^m)$$

$$[F(u^m) : F] = \left[F\left(u^d\right) : F\right] = \frac{n}{d}$$

$$\implies m_{u^m} = x^{n/d} - a^{m/d}$$

■