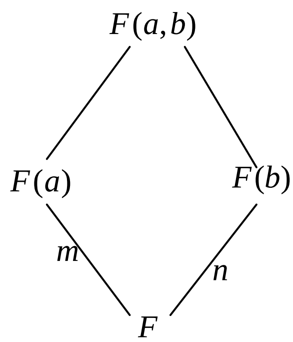
אלגברה מופשטת 3 – תרגול 3

תזכורת: משפט: $F\subset K\subset E\Rightarrow [E:F]=[E:K][K:F]$

תרגיל: אם $a,b\in E\setminus F$ כך ש $[F(a):F]=m,\ [F(b):F]=n$ וגם $(m,n)=1$, אזי $[F(a,b):F]=nm$.

הוכחה:



נסמן $t=[F(a,b):F]$

$$[F(a,b):F]=[F(a,b):F(a)][F(a):F]=m[F(a,b):F(a)]$$
$$[F(a,b):F]=[F(a,b):F(b)][F(b):F]=n[F(a,b):F(b)]$$
$$\Rightarrow t=n[F(a,b):F(b)]=m[F(a,b):F(a)]$$
$$\Rightarrow n\,|\,t,\ m\,|\,t$$
$$\Rightarrow nm\,|\,t$$
$$\Rightarrow nm\le t$$

מצד שני $[F(a,b)=F(a)(b):F(a)]\le n$, כיוון ש $[F(a,b)=F(a)(b):F(a)]=\deg f$ כאשר f הוא הפולינום המינימלי של b מעל $F(a)$. אבל אם g הוא הפולינום המינימלי של b מעל F, אזי $f\,|\,g$, ולכן $[F(a,b):F(a)]=\deg f\le\deg g=[F(b):F]=n$.

תרגיל: יהיו $f(x),g(x)\in F[x]$ פולינומים אי-פריקים כך ש $\deg f=6,\deg g=5$, ונתון $a\in E\setminus F$ שורש של f. הוכיחו או הפריכו: $g(x)$ אי-פריק מעל $F(a)$.

פתרון:

נוכיח. ניתן להניח ש $b\in E$ שורש של g (אחרת נרחיב את E). כעת $[F(a):F]=5,\ \ [F(b):F]=6$. לפי התרגיל הקודם מתקיים $[F(a,b):F]=5\cdot 6=30$. אך מצד שני

$[F(a,b):F]=[F(a,b):F(a)][F(a):F]=6\cdot[F(a,b):F(a)]$. לכן $[F(a,b):F(a)]=5$ ולכן בהכרח g אי-פריק מעל $F(a)$.

תרגיל: יהי $u\in E\setminus F$ עם פולינום מינימלי $m_u(x)=x^n-a$ מעל F. כעת יהי $m\in\mathbb{N}$. מצאו את $m_{u^m}(x)\in F[x]$ הפולינום המינימלי של u^m.

פתרון:

שלב א': נניח ש $m\,|\,n$.

אזי $n=mk$. נחפש פולינום כך ש $f(u^m)=0$.

$0=u^n-a=(u^m)^k-a$ ולכן u^m שורש של $f(x)=x^k-a$.

נניח ש $m_{u^m}(x)=x^t+\sum_{i=0}^{t-1}\alpha_i x^i$. לפי הנ"ל נקבל $t\le k$.

אזי $0=u^{mt}+\sum_{i=0}^{t-1}\alpha_i u^{mi}$, כלומר u שורש של $g(x)=x^{mt}+\sum_{i=0}^{t-1}\alpha_i x^{mi}$ אבל אז בהכרח $mt\ge n$. לכן $t\ge\frac{n}{m}=k$. לכן $t=k$ ו $f=m_{u^m}$.

שלב ב': יהי $d=(m,n)$.

אזי קיימים $s,t\in\mathbb{Z}$ כך ש $sn+tm=d$.

$d\,|\,m\Rightarrow F(u^d)\supseteq F(u^m)$.

נראה ש $F(u^d)\subseteq F(u^m)$: $u^d=u^{sn+tm}=(u^n)^s(u^m)^t=a^s(u^m)^t\in F(u^m)$.

לכן $F(u^d)=F(u^m)$ ולפי שלב א', נקבל $[F(u^m):F]=[F(u^d):F]=\frac{n}{d}$, וגם $m_{u^d}(x)=x^{\frac{n}{d}}-a$.

$(u^m)^{\frac{n}{d}}=(u^n)^{\frac{m}{d}}=a^{\frac{m}{d}}$, ולכן נגדיר $f(x)=x^{\frac{n}{d}}-a^{\frac{m}{d}}$ ואז בהכרח $m_{u^m}(x)=f(x)$.