פתרון תרגיל בית 3 בשדות ותורת גלואה
88-311 סמסטר א' תשפ"ב

שאלה 1 (חימום)**.** תהי K/F הרחבת שדות ממימד ראשוני. יהי $F \subseteq L \subseteq K$ שדה ביניים. הוכיחו $L = F$ או $L = K$.

פתרון. לפי כפליות המימד

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

עבור $[K : F]$ ראשוני. לכן $[L : F] = 1$ או $[K : L] = 1$. כלומר $L = F$ או $L = K$, בהתאמה.

שאלה 2. תהי K/F הרחבת שדות. הוכיחו (למשל באינדוקציה) שלכל $a_1, \ldots, a_n \in K$ מתקיים

$$[F\,[a_1, \ldots, a_n] : F] \leq \prod_{i=1}^{n} [F\,[a_i] : F]$$

פתרון. ראינו שאם $F \subseteq L \subseteq K$ ו-$a \in K$, אז $[L[a] : L] \leq [F[a] : F]$. הרי הפולינום המינימלי של a מעל L מחלק (מעל L) את הפולינום המינימלי של a מעל F. בפרט, אם $L = F[a_1]$ ונספח את a_2 אז

$$[F[a_1, a_2] : F[a_1]] \leq [F[a_2] : F]$$

מכפליות הממד נקבל

$$[F[a_1, a_2] : F] = [F[a_1, a_2] : F[a_1]]\,[F[a_1] : F] \leq [F[a_1] : F]\,[F[a_2] : F]$$

כעת אפשר לעשות אינדוקציה:

$$\begin{aligned}[F\,[a_1, \ldots, a_n] : F] &= [F\,[a_1, \ldots, a_n] : F\,[a_1, \ldots, a_{n-1}]]\,[F\,[a_1, \ldots, a_{n-1}] : F] \\ &\leq [F\,[a_n] : F] \prod_{i=1}^{n-1} [F\,[a_i] : F] = \prod_{i=1}^{n} [F\,[a_i] : F]\end{aligned}$$

שאלה 3. הוכיחו כי $\left[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}\right] = 4$.

הוכחה. ראשית, מתרגיל הבית הקודם אנחנו יודעים כי $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. אפשר להוכיח את הטענה ישירות, על ידי כך שנכתוב בסיס במפורש: $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$. קל לוודא שזו קבוצה פורשת; כדי לוודא שהיא בת"ל מעל $\mathbb{Q}$, ניקח צירוף לינארי מתאפס

$$a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} = 0.$$

נעביר אגפים:

$$\sqrt{3}(a_2 + a_3\sqrt{2}) = -a_0 - a_1\sqrt{2},$$

ולכן

$$.\sqrt{3}=-\frac{a_0+a_1\sqrt{2}}{a_2+a_3\sqrt{2}}$$

נשים לב כי $a_2+a_3\sqrt{2}\neq 0$, כי $\sqrt{2}\notin\mathbb{Q}$, אלא אם $a_2=a_3=0$ (ואז בהכרח גם $a_0=a_1=0$, כנדרש). לכן קיבלנו $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$, בסתירה, אלא אם $a_0=a_1=0$, ואז גם $a_2=a_3=0$.

דרך אחרת, עם כפליות המימד: מתקיים

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

ודאי שמתקיים $\left[\mathbb{Q}(\sqrt{2}):\mathbb{Q}\right]=2$. לחישוב המימד השני, $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3})$; הפולינום המינימלי של $\sqrt{3}$ מעל $\mathbb{Q}(\sqrt{2})$ הוא x^2-3, ולכן $\left[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})\right]=2$. מכפליות המימד נקבל את הנדרש. $\square$

שאלה 4. מצאו את הפולינום המינימלי של האיברים הבאים מעל השדה המצויין:

א. $\sqrt[3]{5}$ מעל $\mathbb{Q}$.

ב. $\sqrt{2}$ מעל $\mathbb{Q}[i]$.

ג. $\sqrt{2+\sqrt{2}}$ מעל $\mathbb{Q}$.

ד. $i+\sqrt{2}$ מעל $\mathbb{Q}$.

פתרון.

א. קל לראות ש-$\sqrt[3]{5}$ מאפס את הפולינום x^3-5, שהוא אי פריק מעל $\mathbb{Q}$ לפי קריטריון אייזנשטיין עבור 5.

ב. x^2-2 מתאפס ב-$\sqrt{2}$. הפולינום המינימלי לא יכול להיות לינארי כי $\sqrt{2}\notin\mathbb{Q}[i]$ (כי אם $\sqrt{2}=a+bi$ אז $bi=\sqrt{2}-a$ הוא ממשי מה שמכריח $b=0$. אבל אז $\sqrt{2}=a\in\mathbb{Q}$ שזו סתירה). לכן x^2-2 הוא הפולינום המינימלי.

ג. נסמן $\alpha=\sqrt{2+\sqrt{2}}$ ונחשב

$$\begin{aligned}\alpha^2&=2+\sqrt{2}\\ \left(\alpha^2-2\right)^2&=2\\ \alpha^4-4\alpha^2+2&=0\end{aligned}$$

ולכן α מאפס את x^4-4x^2+2 שהוא אי פריק לפי אייזנשטיין ולכן זהו הפולינום המינימלי.

ד. נסמן $\alpha=i+\sqrt{2}$ ונחשב

$$\begin{aligned}\alpha^2&=1+2\sqrt{2}i\\ \frac{(\alpha^2-1)^2}{4}&=-2\\ \alpha^4-2\alpha^2+9&=0\end{aligned}$$

לכן x^4-2x^2+9 הוא פולינום מעל $\mathbb{Q}$ שמתאפס ב-α. ניתן להראות ש-$\mathbb{Q}\left[i+\sqrt{2}\right]=\mathbb{Q}\left[i,\sqrt{2}\right]$ ולחשב כי $\left[\mathbb{Q}[i,\sqrt{2}]:\mathbb{Q}\right]=4$. מפני שהפולינום המינימלי צריך להיות ממעלה 4, אז בהכרח הפולינום שמצאנו הוא הפולינום המינימלי.

שאלה 5. תהי K/F הרחבת שדות, ויהי $\alpha \in K$ עם פולינום מינימלי

$$m_\alpha(x) = x^n - c \in F[x]$$

עבור $k \in \mathbb{N}$ מצאו את $m_{\alpha^k}(x)$, הפולינום המינימלי של α^k. הדרכה:

א. הניחו $k|n$ ומצאו פולינום שמתאפס ב-α^k.

ב. למקרה הכללי סמנו $d = (n, k)$ ומצאו קודם את $m_{\alpha^d}(x)$.

פתרון.

א. לפי הנתון קיים q כך ש-$n = kq$. אנחנו יודעים כי

$$0 = \alpha^n - c = (\alpha^k)^q - c$$

ולכן $x^q - c$ הוא פולינום שמתאפס ב-α^k. נניח כי

$$m_{\alpha^k}(x) = x^t + \sum_{i=0}^{t-1} a_i x^i$$

הוא הפולינום המינימלי של α^k וממעלה t. למעשה הראנו $t \leq q$. לפי הגדרה $\alpha^{kt} + \sum_{i=0}^{t-1} a_i \alpha^{ki} = 0$ וקיבלנו ש-α הוא שורש של פולינום ממעלה kt. אז בהכרח $n \leq kt$. כלומר $\frac{n}{k} = q \leq t$, ולכן $t = q$. לכן $m_{\alpha^k}(x) = x^q - c$ הוא ממעלה מינימלית.

ב. קיימים $s, t \in \mathbb{Z}$ כך ש-$d = sn + tk$. לפי הגדרה $d|k$ ולכן $F(\alpha^k) \subseteq F(\alpha^d)$. נרצה להראות הכלה בכיוון השני, ואז להשתמש בסעיף הקודם. נשים לב כי

$$\alpha^d = \alpha^{sn+tk} = (\alpha^n)^s (\alpha^k)^t = c^s (\alpha^k)^t \in F(\alpha^k)$$

ולכן $F(\alpha^k) = F(\alpha^d)$. בעזרת הסעיף הקודם נסיק

$$[F(\alpha^k) : F] = [F(\alpha^d) : F] = \frac{n}{q}$$

וכי $m_{\alpha^d}(x) = x^{n/d} - c$. מפני ש-$(\alpha^k)^{n/d} = (\alpha^n)^{k/d} = c^{k/d}$, נקבל כי $m_{\alpha^k}(x) = x^{n/d} - c^{k/d}$ הוא פולינום שמתאפס ב-α^k עם מעלה השווה לממד ההרחבה, ולכן הוא הפולינום המינימלי.

בהצלחה!