פתרון תרגיל בית 2 תורת גלואה - תשע"ח

1. יהיו $F \subseteq K$ שדות. הוכיחו או הפריכו את הטענות הבאות:

א. אם a איבר אלגברי מעל K אז הוא אלגברי מעל F.

ב. אם a איבר אלגברי מעל F אז הוא אלגברי מעל K.

ג. אם a איבר אלגברי מעל F אז גם $\alpha \cdot a$ הוא אלגברי לכל $\alpha \in F$.

פתרון. א. הפרכה: π הוא אלגברי מעל $K = \mathbb{R}$ (מאפס את הפולינום $x - \pi$) אבל לא מעל $\mathbb{Q}$.

ב. הוכחה: a אלגברי מעל F ולכן יש פולינום $p(x) \in F[x]$ כך ש $p(a) = 0$. אך $F \subseteq K$ ולכן $p(x) \in K[x]$. כלומר שיש פולינום מעל K שמתאפס בa ולכן הוא אלגברי מעל K.

ג. הוכחה: a אלגברי ולכן יש $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ כך ש $p(a) = 0$. אזי

$$0 = p(a) = \frac{1}{\alpha^n}(\alpha a)^n + \frac{1}{\alpha^{n-1}}(\alpha a)^{n-1} + \cdots + \frac{1}{\alpha}(\alpha a) + a_0$$

. נשים לב ש $\frac{1}{\alpha^j}a_i \in F$ וכך $q(x) = \frac{1}{\alpha^n}x^n + \frac{1}{\alpha^{n-1}}x^{n-1} + \cdots + \frac{1}{\alpha}x + a_0$ הוא פולינום מעל F שמתאפס ב αa.

2. הוכיחו כי $\mathbb{Q}\left[i\sqrt{3}\right] = \mathbb{Q}\left[\rho_3\right]$ כאשר $\rho_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ הוא שורש יחידה 3-פרימיטיבי.

פתרון. . קל לראות שהיוצרים מוכלים כל אחד בשדה השני. הייתה טעות בשאלה, השאלה המתוקנת יצאה קלה עד כדי גיחוך.

3. נסמן $\theta = \frac{\sqrt{5}}{2} + \frac{-5}{2}$. חשבו את ההפכי של $\theta^2 + 6\theta + 7$ בשדה $\mathbb{Q}[\theta]$ (חשבו את הפולינום המינימלי. הציגו את ההפכי ע"י נציג מחזקה מינימלית).

פתרון. . נחשב את הפולינום המינימלי:

$$2\theta + 5 = \sqrt{5}$$
$$4\theta^2 + 20\theta + 25 = 5$$
$$\theta^2 + 5\theta + 5 = 0$$

ולכן הפולינום הוא $x^2 + 5x + 5$. זהו אכן הפולינום המינימלי כי הוא מתאפס בθ ואי־פריק מעל $\mathbb{Q}$ (אייזנשטיין בעזרת הראשוני 5).

. נחפש את ההפכי של $x^2 + 6x + 7$ במנה $\mathbb{Q}[x]\big/\langle x^2 + 5x + 5\rangle$:
ראשית נמיר את הנציג ל $\overline{x^2 + 6x + 7} = \overline{x + 2}$.

. ע"י אלגוריתם אוקלידם או ניחוש מושכל ניתן לראות ש $(x + 3)(x + 2) + (-1)(x^2 + 5x + 5) = 1$ ולכן ההפכי הוא $\overline{x + 3}$.

. ולפיכך ההופכי של $\theta^2 + 6\theta + 7$ הוא $\theta + 3$.

4. מצאו את הפולינום המינימלי של האיברים הבאים מעל השדות הנתונים:

א. $\sqrt[3]{5}$ מעל $\mathbb{Q}$.

ב. $\sqrt[4]{3}$ מעל $\mathbb{Q}[\sqrt{3}]$.

ג. $\sqrt{2}$ מעל $\mathbb{Q}[i]$.

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

ה. $\sqrt{x} - 1$ מעל $\mathbb{Q}(x)$.

פתרון. א. $\sqrt[3]{5}$ מאפס את הפולינום $x^3 - 5$ שהוא אי־פריק מעל $\mathbb{Q}$ לפי אייזנשטיין (עבור 5).

ב. $\sqrt[4]{3}$ מאפס את x^4-3. מעל $\mathbb{Q}[\sqrt{3}]$ הפולינום הזה מתפרק ל $(x^2-\sqrt{3})(x^2+\sqrt{3})$ כאשר הרכיב $x^2-\sqrt{3}$ מתאפס ב$\sqrt[4]{3}$.
הפולינום המינימלי הוא בודאי לא לינארי כי $\sqrt[4]{3}\notin\mathbb{Q}[\sqrt{3}]$ (לא יכול להיות $\sqrt[4]{3}=a+b\sqrt{3}$ כי אנחנו יודעים ש $1,\sqrt[4]{3},\left(\sqrt[4]{3}\right)^2=\sqrt{3},\left(\sqrt[4]{3}\right)^3$ הם בת"ל מעל $\mathbb{Q}$ לפי השדה $\mathbb{Q}[\sqrt[4]{3}]$) ולכן הפולינום המינימלי הוא $x^2-\sqrt{3}$.

ג. 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 $\sqrt{2}-a=bi$ הוא ממשי מה שמכריח $b=0$. ואז $\sqrt{2}=a\in\mathbb{Q}$ וקיבלנו סתירה).

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

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

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

ה. נסמן $\alpha=\sqrt{x}-1$ אזי

$$(\alpha-1)^2=x$$
$$\alpha^2-2\alpha+(1-x)=0$$

ולכן αמאפס את הפולינום $\lambda^2-2\lambda+(1-x)$. הפולינום המינימלי לא יכול להיות לינארי ($\sqrt{x}\notin\mathbb{Q}(x)$ משיקולי דרגות) ולכן זהו הפולינום המינימלי.

5. כמה תת־שדות של $\mathbb{C}$ איזומורפיים ל$\mathbb{Q}\left[\sqrt{2+\sqrt{2}}\right]$?

פתרון. . נראה שיש רק שדה אחד כזה.

. ראינו בשאלה הקודמת שהפולינום המינימלי של $\sqrt{2+\sqrt{2}}$ מעל $\mathbb{Q}$ הוא x^4-4x^2+2.

השורשים של הפולינום הזה ב$\mathbb{C}$ הם $\pm\sqrt{2\pm\sqrt{2}}$ ולכן

$$\mathbb{Q}\left[\sqrt{2+\sqrt{2}}\right] \cong \mathbb{Q}\left[-\sqrt{2+\sqrt{2}}\right] \cong \mathbb{Q}\left[\sqrt{2-\sqrt{2}}\right] \cong \mathbb{Q}\left[-\sqrt{2-\sqrt{2}}\right]$$

הם כל השדות שאיזומורפיים לשדה הנתון.

- קל לראות ש $\mathbb{Q}\left[\sqrt{2+\sqrt{2}}\right] = \mathbb{Q}\left[-\sqrt{2+\sqrt{2}}\right]$
- ו $\mathbb{Q}\left[\sqrt{2-\sqrt{2}}\right] = \mathbb{Q}\left[-\sqrt{2-\sqrt{2}}\right]$.
- $\sqrt{2} = \left(\sqrt{2+\sqrt{2}}\right)^2 - 2 \in \mathbb{Q}\left[\sqrt{2+\sqrt{2}}\right]$ ואז $\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \in \mathbb{Q}\left[\sqrt{2+\sqrt{2}}\right]$.

6. יהיו שדות $K_1, K_2 \subseteq L$ נוכל להגדיר את הקומפוזיטום שלהם K_1K_2 כתת־שדה של L המינימלי שמכיל את K_1 ואת K_2.
נניח $K_1 = F(a_1, \ldots, a_n)$ ו $K_2 = F(b_1, \ldots, b_m)$ הוכיחו כי $K_1K_2 = F(a_1, \ldots, a_n, b_1, \ldots, b_m)$.

פתרון.

- מצד אחד $K_1, K_2 \subseteq F(a_1, \ldots, a_n, b_1, \ldots, b_m)$ ולכן $K_1K_2 \subseteq F(a_1, \ldots, a_n, b_1, \ldots, b_m)$ כי הקומפוזיטום מינימלי.
- מצד שני, $K_1, K_2 \subseteq K_1K_2$ ולכן $F, a_1, \ldots, a_n, b_1, \ldots, b_m$ שייכים ל K_1K_2 ולכן $F(a_1, \ldots, a_n, b_1, \ldots, b_m) \subseteq K_1K_2$ (כי זה השדה המינימלי שמכיל את F וכל האיברים a_i, b_j).
- ולכן יש שיוויון.

7. תהי K/F הרחבה ממימד סופי. הוכיחו כי כל איבר של K הוא אלגברי מעל F (במצב כזה אומרים שK/F הרחבה אלגברית).
(רמז: חשבו על החזקות $1, a, a^2, a^3, \ldots$).

פתרון.

- יהי $a \in K$, מכיוון שהמימד סופי הקבוצה $\{1, a, a^2, \ldots\}$ חייבת להיות תלויה לינארית מעל F כלומר שיש צירוף לינארי לא טריוויאלי של החזקות שמתאפס:

. $b_na^n+b_{n-1}a^{n-1}+\cdots+b_0=0$ ולכן $b_nx^n+\cdots+b_0\in F[x]$ הוא פולינום שמתאפס ב־a ולכן a אלגברי מעל F.

8. תהי $K/_F$ הרחבה ממימד סופי. נקבע איבר $a\in K$ ונסמן את הפולינום המינימלי שלו מעל F ב $f_a(x)$ (שבודאי קיים לפי השאלה הקודמת).
נתבונן בפונקציה $l_a\colon K\to K$ המוגדרת ע"י $l_a(k)=ak$. זוהי העתקה לינארית של המ"ו K מעל F.
נסמן את הפולינום האופייני של l_a (בתור העתקה לינארית) ב$g(x)$.
הוכיחו כי $f_a(x)\mid g(x)$ מעל F.
(רמז: קיילי המילטון)

פתרון. . לפי קיילי־המילטון $g(l_a)=0$ (זהו שיוויון של העתקות לינאריות!).

. אם נרשום $g(x)=x^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0$ אזי $l_a^n+b_{n-1}l_a^{n-1}+\cdots+b_1l_a+b_0Id=0$.

. נפעיל את ההעתקה הלינארית הזאת על 1:

$$(l_a^n+b_{n-1}l_a^{n-1}+\cdots+b_1l_a+b_0Id)(1)=0(1)$$
$$a^n+b_{n-1}a^{n-1}+\cdots+b_1a+b_0=0$$

שימו לב ש $l_a^n(1)=\underbrace{l_a\circ l_a\circ\cdots\circ l_a}_{n}(1)=\underbrace{l_a\circ l_a\circ\cdots\circ l_a}_{n-1}(a\cdot 1)=\underbrace{l_a\circ l_a\circ\cdots\circ l_a}_{n-2}(a^2)=\cdots=a^n$.

. אם כן $g(x)$ הוא פולינום מעל F המתאפס בa ולכן הפולינום המינילי מחלק אותו : $f_a(x)\mid g(x)$.

הערה לשים לב שהשאלה הזו היא הוכחה נוספת לכך שאם המימד הוא סופי אז כל איבר הוא אלגברי־ שהרי בגלל שהמימד היה סופי (זה היה קריטי! איפה?) מצאנו פולינום שמתאפס בa והוא הפולינום האופייני של ההעתקה l_a.